StorageTek Tape Analytics

Installation and Configuration Guide

Release 2.0.1

E41585-02

June 2014

ORACLE

StorageTek Tape Analytics Installation and Configuration Guide, Release 2.0.1

E41585-02

Primary Author: Kristofer Vickland

Contributing Authors: Nancy Stevens, Greg Barnes

Contents

Preface

This document describes installing and configuring Oracle's StorageTek Tape Analytics (STA). Review the following sections before deploying STA.

STA Deployment Overview

To install and configure STA, you perform the following tasks. See "Audience" to determine which tasks and associated chapters are applicable to your role. You can perform the installation yourself or purchase Oracle installation services.

Note: If you are upgrading STA, see Chapter 9, "Upgrading STA."

Task	Description	Location
1	Review STA requirements	*STA Requirements Guide*
2	Submit Service Request(s)	"Prepare Service Requests for Oracle Support" on page 2-viii
3	Install and configure Linux	Chapter 1, "Installing Linux"
4	Install STA	Chapter 2, "Installing STA"
5	Configure libraries	Chapter 3, "Library Configuration Concepts" Chapter 4, "Library Configuration Process"
6	Configure STA	Chapter 5, "Configuring SNMP in STA" Chapter 6, "Configuring Users and Email"
7	Configure STA services (recommended)	Chapter 7, "Configuring STA Services"
8	Configure certificates (optional)	Chapter 8, "Configuring Certificates"
9	Configure SSP authentication (optional)	Appendix A, "Configuring a SSP for STA"

Prepare Service Requests for Oracle Support

Use this procedure and the referenced sections to provide Oracle Support with the information needed to prepare your library for monitoring. If STA will be monitoring a library complex, prepare a service request for each library in the complex. Additionally, open a Service Request to obtain the latest drive firmware supported by STA.

1. **Verify the library firmware version**: See "Verify the Library Firmware Version" on page 4-3.
2. **Verify a high-memory HBT card is installed (SL3000 and SL8500 only)**: See "Verify the Drive Controller Card Version (SL3000 and SL8500 Only)" on page 4-5.
3. **Enable ADI on library and LTO drives**: For libraries with LTO drives only. See the *STA Requirements Guide* for more information.
4. **Set the library complex ID (SL8500 only)**: See "Ensure the Correct Library Complex ID (SL8500 Only)" on page 4-13.
5. **Set the library date and time**: To ensure that library data date/time stamps correlate to STA server date/time stamps, the library clock should be set appropriately by Oracle Support.
6. **Submit the service request(s).**

Audience

This document is intended for the following audiences:

- **Linux Admin**: Installs, configures, and administers Linux on the STA server.
- **STA Admin**: Installs, configures, and administers STA.
- **Library Admin**: Configures and administers StorageTek libraries.
- **MVS System Programmer**: Configures and administers IBM mainframes.

Chapter	Audience
Chapter 1, "Installing Linux"	Linux Admin
Chapter 2, "Installing STA"	STA Admin
Chapter 3, "Library Configuration Concepts"	Library Admin
Chapter 4, "Library Configuration Process"	Library Admin
Chapter 5, "Configuring SNMP in STA"	STA Admin
Chapter 6, "Configuring Users and Email"	STA Admin
Chapter 7, "Configuring STA Services"	STA Admin
Chapter 8, "Configuring Certificates"	STA Admin
Chapter 9, "Upgrading STA"	STA Admin Linux Admin
Chapter 10, "Uninstalling and Reinstalling STA"	STA Admin
Appendix A, "Configuring a SSP for STA"	STA Admin MVS System Programmer
Appendix B, "Configuring SNMP v2c Mode"	Library Admin STA Admin
Appendix C, "Configuration Troubleshooting"	Library Admin STA Admin

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

- *STA Release Notes*[1]
- *STA Requirements Guide*
- *STA Administration Guide*
- *STA Quick Start Guide*
- *STA Screen Basics Guide*
- *STA User's Guide*
- *STA Data Reference Guide*
- *STA Security Guide*
- *STA Third Party Licenses and Notices*

Library and tape drive documentation can be found on the Oracle Technology Network website:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

[1] Included with the STA media pack download.

What's New

This book has been updated with the following major changes since the initial STA 2.0 release.

Chapter 1, "Installing Linux"

- Added post-installation task to check for allowance of "install" user and group creation

Chapter 9, "Upgrading STA"

- Added content for upgrading STA 2.0 to 2.0.x
- Modified content for upgrading STA 1.0.x to 2.0.x

1 Installing Linux

Before installing Linux on the STA server, review the system requirements in the *STA Requirements Guide*.

> **Note:** You cannot perform an in-place upgrade of Linux 5.x to Linux 6.x. If you are installing Linux 6.x as part of an upgrade to STA 2.0.x, consult Chapter 9, "Upgrading STA."

To install and configure Linux for STA, perform the tasks in Table 1–1.

Table 1–1 Linux Installation Tasks

Category	Task
Preparation	Task 1, "Review Related Documentation" Task 2, "Download the Linux Installer Media Pack"
Installation	Task 1, "Gather Required Information" Task 2, "Install Linux" Task 3, "Run the Linux Setup Agent"
Post-Installation	Task 1, "Disable SELinux" Task 2, "Disable the Linux Firewall" Task 3, "Disable Access Control" Task 4, "Set Up the Network Proxy" Task 5, "Ensure Proper Setup of yum" Task 6, "Install Required Linux Packages" Task 7, "Ensure Proper Setup of SSH" Task 8, "Ensure Proper DNS Settings" Task 9, "Disable Name Service(s)" Task 10, "Ensure User and Group Creation Allowed" Task 11, "Ensure Local Browser Functionality (Optional)"

1.1 Preparation

Task 1 Review Related Documentation

Due to the wide variety of network configuration requirements and options, refer to the following documents for help with installing and configuring the hardware,

software, and network. IPv4 and IPv6 network configuration are discussed in detail in these documents.

- Oracle Linux Installation Guides:

  http://www.oracle.com/technetwork/topics/linux/index-099698.html

- RedHat Linux Documentation:

  http://docs.redhat.com/docs/en-US/index.html

Task 2 Download the Linux Installer Media Pack

You must obtain Oracle Linux from the Oracle Software Delivery Cloud website. If you do not have a user ID and password, contact Oracle Support.

1. Navigate to the Oracle Software Delivery Cloud website:

   http://edelivery.oracle.com/linux

2. Click **Sign In/Register**.
3. Enter the user ID and password provided by Oracle Support.
4. On the Terms & Restrictions screen, select the boxes to indicate your acceptance of the License Agreement and Export Restrictions, and then click **Continue**.
5. On the Media Pack Search screen:
   a. In the Select a Product Pack menu, select **Oracle Linux**.
   b. In the Platform menu, select **x86 64** bit (STA requires 64-bit Linux).
   c. Click **Go**.
6. Select a Linux version, and then click **Continue**.

   For Linux version requirements, see the *STA Requirements Guide*.
7. Click **Download** for the 64-bit option.
8. Save the ISO file and write it to media.

1.2 Installation

The following procedures assume an Oracle Enterprise Linux (OEL) 6u4 DVD installation with graphical installer and setup agent. If you install a different version of Linux, use different media, or use the console mode, the steps and packages may vary.

Task 1 Gather Required Information

Check with your system administrator to obtain:

- Hostname and IP address for the STA server
- Gateway IP address and netmask for your network
- DNS server IP addresses and search domains for your network
- IP address of the NTP (network time protocol) servers you will be using
- Network proxy information, if applicable

Task 2 Install Linux

1. Connect the installation media to the STA server.
2. Start the Linux installer using the instructions in the README file on the media.

3. Select **Install or upgrade an existing system**.
4. If you are installing from a DVD, the CD Found screen appears. You can optionally perform a test of the media. To skip the test, press **Tab** to highlight the **Skip** option, and then press **Spacebar**.
5. On the Welcome screen, click **Next**.
6. Select a language, and then click **Next**.
7. Select a keyboard layout, and then click **Next**.
8. Select **Basic Storage Devices**, and then click **Next**.
9. Enter a hostname for the STA server, and then click **Configure Network**.
10. Select the network adapter name, and then click **Edit**.
11. Ensure that **Connect automatically** and **Available to all users** are both selected.
12. In the remaining tabs, configure the adapter as per your network administrator's IPv4 or IPv6 specifications. You must specify a static IP address for the STA server, and at least one DNS server. When done, click **Apply**, **Close**, and **Next**.
13. Select the STA server's time zone, select the **System clock uses UTC** check box, and then click **Next**.
14. Enter and confirm a root password for the server, and then click **Next**.
15. Identify a partitioning layout to use on the server:
    a. Because STA requires a dedicated server, Oracle recommends selecting **Use All Space**.
    b. Select the **Review and modify partitioning layout** check box, and then click **Next**.
16. Use Table 1–2 to modify the filesystem layout, as the default does not meet the minimum requirements for STA[1]. When done, click **Next**.

> **Note:** Oracle recommends creating all of these filesystems in advance of installing STA; otherwise, STA will be installed in the "/" and /var directories, requiring additional space allocation to those directories. While the STA installer will create directories as needed, you will have greater control of filesystem properties if you create them in advance.

[1] Alternately, you can modify the filesystem after Linux installation with the **system-config-lvm** utility.

Table 1–2 Recommended Filesystem Structure

Filesystem	Directories/ Mountpoints	Size	Purpose	Recommendations
root	/	32 GB minimum	/tmp files	If /tmp is contained on this filesystem, a minimum of 4 GB of free space should be maintained. This space is required during STA installations and upgrades.
STA Oracle	/Oracle	20 GB minimum 30 GB optimum	STA application	This should be a separate filesystem on a separate volume. Maintain a minimum of 4 GB free space for STA installations and upgrades. Maintain an additional 5 GB free space for WebLogic log rotation. STA creates the following Oracle Middleware subdirectories: ▪ Rotated WebLogic logs: /Oracle/Middleware/user_projects/domains/tbi/servers ▪ RDA last CLI snapshot: /Oracle/Middleware/rda/output ▪ STA GUI snapshot log bundles: /Oracle/Middleware/rda/snapshots
swap	None	1/2X-1X RAM	Swap space	None. Defined as memory.
STA var	/var/log/tbi	10 GB minimum 50 – 100 GB optimum	STA logs	This should be a separate volume at this mount point. Content is managed through log rotation. **Note**: Except for log rotation, STA does not perform space management. **Caution**: You must configure the STA backup utility to manage the log files in /var/log/tbi/db/stadb_bin. Otherwise, these files may require manual management (see "MySQL Binary Logs" in the *STA Administration Guide*).
STA_DB	/dbdata	250 GB – 2 TB	STA database	Oracle highly recommends you place this directory on its own volume, separate from /root, /swap, /Oracle, and /var, on separate mirrored or striped drives. Required size depends on the number of libraries, drives, media, exchanges per day, and historical years of data. Oracle recommends that you configure STA services to alert if space utilization exceeds a specified percentage.
STA_DB local backup	/dbbackup	60-70% of /dbdata	STA last local DB backup	This should be on a different volume from /dbdata, and on mirrored or striped drives, in case of database corruption or failure.

17. When ready, select **Write changes to disk**.
18. In the boot loader screen, leave all options as-is, and then click **Next**.
19. In the software selection screen, select **Basic Server**, and do not change the repository options. Then, select **Customize now**, and then click **Next**.
20. In the package selection screen, use Table 1–3 to configure the packages for each package category:
    a. Select a package category.
    b. Select the box for each package in the Select column.
    c. If a package requires an option (indicated with a +), highlight the parent package, click the **Optional packages** button, select the child package in the list, and then click **Close**.
    d. Deselect the box for each package in the Deselect column.
    e. Leave other check boxes as-is.

Table 1–3 Linux Package Selection

Package Category	Select	Deselect
Base System	▪ Base ▪ Compatibility libraries ▪ Console internet tools ▪ Java Platform ▪ Legacy UNIX compatibility + `ksh-xxxxxxxx-xx.el6.x86_64`	▪ Debugging Tools ▪ Dial-up Networking Support ▪ Directory Client ▪ Hardware monitoring utilities ▪ Large Systems Performance ▪ Network file system client ▪ Performance Tools
Servers	▪ System administration tools[1]	NA
Web Services	NA	All packages
Databases	NA	All packages
System Management	NA	NA
Virtualization	NA	NA
Desktops[2]	▪ Desktop ▪ Desktop Platform ▪ General Purpose Desktop ▪ Graphical Administration Tools + `system-config-lvm-x.x.xx-xx.el6.noarch`[3] ▪ Legacy X Window System compatibility ▪ X Window System	NA
Applications	▪ Internet Browser[4]	NA
Development	▪ Development tools + `expect-x.xx.x.xx-x.el6.x86_64`	NA
Languages	NA	NA

[1] Optional.
[2] Recommended. Used to perform certain post-installation steps in a graphical environment, as documented later in this chapter.
[3] Optional. Can be used to configure or re-configure the filesystem once Linux installation is complete.
[4] Optional. Can be used to locally configure and manage the STA server with the GUI interface.

21. When you are finished with package selection, click **Next**. Installation will begin.

    If you accidentally click **Next** before configuring all the packages, click **Back** after the software completes a dependency check.

22. When the Congratulations screen appears, remove the installation media, and then click **Reboot**.

    A complete log of the installation can be found in /root/install.log.

Task 3 Run the Linux Setup Agent

The Linux Setup Agent starts automatically when you reboot the Linux server.

1. On the Welcome screen, click **Forward**.
2. Read the License Agreement, select **Yes, I agree to the License Agreement**, and click **Forward**.
3. On the Software Updates screen, if you'd like to register your system for updates, select **Yes, I'd like to register now**. Otherwise, select **No, I prefer to register at a later time**, and click **Forward**.
4. On the Finish Updates Setup screen, click **Forward**.

5. On the Create User screen, leave the fields blank, click **Forward**, and then **Yes** to continue. The STA server does not require a non-administrative user.
6. In the Date and Time screen:
   a. Set the current date and time.
   b. Select the **Synchronize date and time over the network** check box.
   c. Add or remove the desired NTP servers (obtained from your IT administrator), and then click **Forward**.

   Note: To ensure that STA data and log files are correct, the date and time on the STA server must be correct. Additionally, any library connected to STA must also have the correct time.
7. On the Kdump screen, do *not* select **Enable kdump?**, and then click **Finish**.

   The system will reboot.
8. After the system reboots, log in as the root user:
   a. Click **Other...**.
   b. Enter username **root**, and then click **Log In**.
   c. Enter the root password, and then click **Log In** again.

      If a message appears about being logged in as root super user, you may ignore the message.
9. (Optional) You can confirm the Linux release and update level by issuing the following command:

```
# cat /etc/issue
Oracle Linux Server release 6.4
Kernel \r on an \m
```

1.3 Post-Installation

Task 1 Disable SELinux

Oracle recommends disabling SELinux on the STA server.

1. Open a terminal session on the STA server.
2. Open the SELinux configuration file with a text editor.

```
# vi /etc/sysconfig/selinux
```

3. In the file, set **SELINUX** to **disabled**:

```
SELINUX=disabled
```

4. Save and exit the file.

Task 2 Disable the Linux Firewall

Oracle recommends disabling the firewall on the STA server. However, you may choose to enable and configure the firewall depending on your site requirements.

To disable the firewall:

1. Open a terminal session on the STA server.

2. Check the settings of the Linux firewall (for next boot) by issuing the following command:

```
# chkconfig --list |grep "ip"
```

If the firewall is set to be disabled on next boot, all output for both iptables and ip6tables will show as **off**. If this is not the case, disable the firewall:

```
# chkconfig iptables off
# chkconfig ip6tables off
```

3. Check the current status of the Linux firewall by issuing the following commands:

```
# service iptables status
# service ip6tables status
```

The command output will indicate if the firewall is currently running. If the firewall is running, stop the firewall:

```
# service iptables stop
# service ip6tables stop
```

4. If either of the following is true, you will need to reboot the server.
   - You disabled SELinux in Task 1.
   - You disabled the Linux firewall (using **chkconfig**) in this section.

Task 3 Disable Access Control

Access control must be disabled for certain directories.

1. Execute the `ls -ld` command for the /Oracle, /dbbackup, /dbdata, and /var/log/tbi directories.

```
# ls -l directory-name
```

For example:

```
# ls -ld /Oracle
drwxr-xr-x 5 root root 4096 Mar 11 15:09 /Oracle

# ls -l /dbbackup
drwxr-xr-x 5 root root 4096 Aug  8  2013 /dbbackup
```

2. In the output for each command, look for a dot at the end of the stated permissions. In the below example, note the "." after `drxwr-xr-x`:

```
# ls -l /Oracle
drxwr-xr-x.  5  root  root  4096  Mar  17  18:27  /Oracle
```

3. If none of the directories contain a period after the permissions statement, access control is already disabled, and you can skip to the next task. If access control is enabled on a directory, as root, execute the following command for that directory:

```
# setfattr -h -x security.selinux directory-name
```

For example:

```
# setfattr -h -x security.selinux /Oracle
```

Task 4 Set Up the Network Proxy

You can configure the STA server to connect to the network directly or through a proxy server.

1. From the Linux desktop, select **System** > **Preferences** > **Network Proxy**.
2. In the Network Proxy Preferences dialog box, specify the proxy configuration per your site requirements.
3. Click **Close**.

Task 5 Ensure Proper Setup of yum

Yum (Yellowdog Updater, Modified) is used for managing software package updates. Use this procedure to ensure that yum is configured correctly on the STA server.

The following command examples use the yum repository for Oracle Linux. In these commands, the "l" in "ol6" is lowercase 'L'.

> **Note:** This procedure assumes you can reach Oracle's public yum server. If your network firewall prohibits external network access, you can install locally available packages from the Linux media. For example:
>
> ```
> # cd /mnt/install-media-mount-location/packages
> # yum install ./package-name
> ```

1. Ping the Oracle public-yum server to ensure the network connection is working.

   ```
   # ping public-yum.oracle.com
   ```

2. Change to the yum repository directory and determine the yum repository filename.

   ```
   # cd /etc/yum.repos.d
   # ls
   public-yum-ol6.repo
   ```

3. Remove the existing yum repository file.

   ```
   # rm public-yum-ol6.repo
   ```

4. Download the latest yum repository file from the yum website.

   ```
   # wget http://public-yum.oracle.com/public-yum-ol6.repo
   ```

   > **Note:** Subsequent executions of this command will copy a new repository file into the yum.repos.d folder with a new extension (for example, public-yum-ol6.repo.1). However, yum always uses the repository file with no extension.

5. Open the repository file with a text editor.

   ```
   # vi public-yum-ol6.repo
   ```

6. In the file, locate the entry that matches your Linux version and enable it by setting **enabled=1**. Disable all other entries by setting **enabled=0**.

   For example:

   ```
   [Linux_Version]
   name=Oracle Linux $releasever Update x installation media copy ($basearch)
   baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL6/x/base/$basearch/
   gpgkey=http://public-yum.oracle.com/RPM-GPG-KEY-oracle-ol6
   ```

```
gpgcheck=1
enabled=1
```

7. Save and exit the file.

Task 6 Install Required Linux Packages

Additional packages are required for STA installation and operation. The STA installer will check for these packages — if they are not present, STA installation will fail.

Depending on your specific Linux installation, some of these packages may have already been installed. If a package is already installed and at the most current version, the system will notify you.

> **Note:** The command used to install the packages will check for and install the most current version (and any dependencies) for your specific Linux version.

To install the packages, do the following.

1. Open a terminal session on the STA server.
2. Issue the following command:

   ```
   # yum install package_name
   ```

   The package will be downloaded and checked. Follow the prompts to install the package. Repeat this step for each of the following packages:

❑ binutils	❑ gcc-c++	❑ libstdc++
❑ compat-libcap1	❑ glibc	❑ libstdc++-devel
❑ compat-libstdc++-33.i686	❑ glibc-devel	❑ net-snmp-utils
❑ cronie	❑ libaio	❑ rpm-build
❑ expect	❑ libaio-devel	❑ sysstat
❑ gcc	❑ libgcc	

Task 7 Ensure Proper Setup of SSH

Use this procedure to ensure that SSH (secure shell) is set up correctly on the STA server. This will speed up transfers of STA database backups to a remote host.

1. Open the SSH configuration file with a text editor.

   ```
   # vi /etc/ssh/sshd_config
   ```

2. Search for the AddressFamily and UseDNS entries. Modify them so they are *not* preceded with the comment character and their values are as follows:

   ```
   AddressFamily inet
   UseDNS no
   ```

3. Save and exit the file.
4. Restart the sshd daemon.

   ```
   # service sshd restart
   ```

Task 8 Ensure Proper DNS Settings

Use this procedure to ensure that the STA server's IP address is mapped to its hostname.

1. Open the hosts file with a text editor.

   ```
   # vi /etc/hosts
   ```

2. At the end of the file, add the STA server's IP address, followed by a tab, and then the STA server's hostname. For example:

   ```
   127.0.0.1    localhost localhost.localdomain localhost4...
   ::1          localhost localhost.localdomain localhost6...
   192.0.2.20    sta_server
   ```

3. Save and exit the file. You do not need to restart the STA server for the new setting to take effect.

Task 9 Disable Name Service(s)

Name services such as LDAP can conflict with STA installation. Use this procedure to temporarily disable these services.

1. Open the Name Service Switch config file with a text editor.

   ```
   # vi /etc/nsswitch.conf
   ```

2. Disable any name service entries. For example, to disable LDAP, comment out "ldap" from the following lines as shown:

   ```
   passwd:     files #ldap nis nisplus
   shadow:     files #ldap nis nisplus
   group:      files #ldap nis nisplus
   ```

3. Save and exit the file. You do not need to restart the STA server for the new setting to take effect. After you install STA, you can modify the nsswitch.conf file to re-enable the name services.

Task 10 Ensure User and Group Creation Allowed

During STA installation, a temporary local user and group, "install", will be created. If this fails for any reason (for example, due to site security policies), then the installation will fail. Use the following procedure to ensure that this user and group can successfully be created.

1. Check the user and group definition files for "install".

   ```
   #  grep "install" /etc/passwd /etc/group
   ```

   Expected result: Neither user nor group should exist (no results are returned).

2. Test that the "install" user and group can be created.

   ```
   # useradd install
   # grep "install" /etc/passwd /etc/group
   ```

   Example output:

   ```
   /etc/passwd:install:x:501:501::/home/install:/bin/bash
   /etc/group:install:x:501:
   ```

   If either the user or group was not created, investigate your site for the failure reason.

3. Remove "install" prior to installing STA.

```
# userdel install
```

Task 11 Ensure Local Browser Functionality (Optional)

To configure and administer STA locally on the STA server, ensure you have the minimum supported browser versions and plugins installed (see the *STA Requirements Guide*).

Note: Oracle does not recommend local access to the STA application due to server performance degradation.

2

Installing STA

This chapter details the STA download and installation process, and assumes you are installing STA for the first time. If you are upgrading STA, consult Chapter 9, "Upgrading STA" (Oracle recommends you install or upgrade to the latest version of STA). If you need to uninstall or reinstall STA, see Chapter 10, "Uninstalling and Reinstalling STA."

> **Note:** Oracle will provide support only if STA is installed on a server dedicated to STA.

2.1 Installation Checks

The STA installer will check that the following conditions are true for your environment. Contact your Linux administrator if you are unsure of the status of these items.

❑ **Existing software is removed**

The installer will check your environment for existing software and settings:

- If the installer detects software in the /Oracle/Middleware directory, allow the installer to remove and reinstall it.
- If the installer detects an existing MySQL installation, allow the installer to remove it.
- If you are prompted to overwrite existing files, allow the installer to do so.

> **Caution:** Before choosing to permanently remove or replace existing software, back up files as needed.

❑ **64-bit Linux is installed with the required packages**

See the *STA Requirements Guide* for supported operating systems. The installer will also check for the required Linux packages mentioned in Chapter 1, "Installing Linux."

- ❏ **SELinux is disabled**

  Oracle highly recommends you disable SELinux before installing STA. If Linux was installed as instructed in Chapter 1, "Installing Linux," SELinux should already be disabled.

- ❏ **Linux firewall (IPTables) is stopped**

  Oracle highly recommends you stop IPTables before installing STA. If Linux was installed as instructed in Chapter 1, "Installing Linux," IPTables should already be stopped. Once you install STA, configure the libraries, and confirm STA is monitoring the libraries successfully, you can enable IPTables. Then, ensure that STA is successfully monitoring the libraries after enabling IPTables.

- ❏ **SNMP services are deconfigured and stopped**

  To avoid network port collisions and other issues, the STA platform must not run other SNMP services:

  - The installer will check to see if snmpd and snmptrapd are running on your system. You must stop and deconfigure these services before installing STA.
  - The installer will also check to ensure that UDP ports 161 (SNMP) and 162 (SNMPTRAP) are available. If they are not, the installer will quit.

  To check the status of, deconfigure, and stop typical SNMP daemon and SNMP trap daemon services, you can issue the following commands:

  - Check the status of SNMP services:

    ```
    # service snmpd status
    # service snmptrapd status
    # chkconfig --list snmpd
    # chkconfig --list snmptrapd
    ```

  - Deconfigure SNMP services:

    ```
    # chkconfig snmpd off
    # chkconfig snmptrapd off
    ```

  - Stop SNMP services:

    ```
    # service snmptrapd stop
    # service snmpd stop
    ```

  Note: If you receive a "FAILED" error when executing the "service stop" commands, these SNMP services may already be stopped.

2.2 User Accounts

The following accounts are required and established during STA installation. These account usernames are STA-specific; they are *not* Linux/Unix users. After installation, additional user accounts with assignable roles can be created within the STA UI, as described in Chapter 6, "Configuring Users and Email."

WebLogic accounts (Table 2–1) are used to access either the WebLogic administration console or the STA UI with a web browser, while database accounts (Table 2–2) are used by STA to manage the STA database.

Username Requirements

- At least one character, with a maximum of 16 characters
- All usernames must be unique

Password Requirements

- Must contain more than seven characters and less than 32 characters
- Cannot contain spaces
- Must contain at least one number or special character, except:

  & ( ) < > ? {}*\`"

Table 2–1 WebLogic Accounts

Account	Description	Username	Password
Admin Console Login	Use to log in to the WebLogic console to make changes to the WebLogic environment (for example, to connect WebLogic to an LDAP or RACF server). **CAUTION**: The Admin Console Login username and password are not retrievable. If these credentials are lost, STA must be re-installed.		
STA GUI Login	Use to log in to the STA GUI application.		

Table 2–2 MySQL Database Accounts

Account	Description	Username	Password
Root Account	Owns the MySQL database and is used to create the root DB installation. The pre-set username is `root` and cannot be changed. **CAUTION**: The database root account password is not retrievable.	`root`	
Application Account	A user-defined MySQL username (for example, `staapp`) that STA uses to connect to the database. It is required to create, update, delete, and read privileges on data tables.		
Reports Account	A user-defined MySQL username (for example, `starpts`) that non-STA and third-party applications may use to connect to the database. It has read-only access to certain database tables.		
DBA Account	A user-defined MySQL username (for example, `stadba`) that STA administration and monitoring utilities use to connect to the database to primarily configure and run scheduled backups. It has all DBA privileges except the “grant option” on all database tables.		

2.3 Port Configuration

STA uses the following ports to retrieve and receive data. During installation, you will be asked to choose values for the configurable ports described below. All port values must be unique.

Caution: Once you select the configurable port values during STA installation, they cannot be changed without uninstalling and reinstalling STA. If you are unsure about what port numbers to choose, contact your network administrator.

Unconfigurable External Ports

These ports (Table 2–3) are used for communication between the STA server and other network entities and cannot be changed during installation.

Firewall/router configuration: Open between the STA server and backup server (for SSH) and between the STA server and libraries (for SNMP and SNMPTRAP).

Table 2–3 Unconfigurable External Ports

Port	Protocol	Description/Purpose
22	SSH	Secure Shell. STA database backup; library log-in.
161	SNMP	Simple Network Management Protocol (SNMP). For transmittal of SNMP requests.
162	SNMPTRAP	For reception of SNMP notifications (traps).

Configurable External Ports

These ports (Table 2–4) are used for communication between the STA server and other network entities, and can be changed during STA installation. They must remain available and dedicated to STA.

Firewall/router configuration: Open between the STA server and the client running the STA GUI.

Table 2–4 Configurable External Ports[1]

Default Port	Your Port	Protocol	Description/Purpose
7001		HTTP	Access to the WebLogic Admin Console, unsecure
7002		HTTPS	Access to the WebLogic Admin Console, secure
7021		HTTP	staUi managed server. Access to the STA GUI, unsecure.
7022		HTTPS	staUi managed server. Access to the STA GUI, secure.

[1] These ports are the configurable equivalent of standard ports 80 and 8080 (HTTP) and 443 (HTTPS), and must be unique from other HTTP and HTTPS ports on the network.

Configurable Internal Ports

These ports (Table 2–5) are used internally by STA and can be changed during STA installation.

Firewall/router configuration: NA

Table 2–5 Configurable Internal Ports

Default Port	Your Port	Protocol	Description/Purpose
7023		HTTP	staEngine managed server. Basic STA internals, unsecure.
7024		HTTPS	staEngine managed server. Basic STA internals, secure.
7025		HTTP	staAdapter managed server. SNMP communication, unsecure.
7026		HTTPS	staAdapter managed server. SNMP communication, secure.

2.4 Download STA

1. Go to the Oracle Software Delivery Cloud website:

http://edelivery.oracle.com/

2. Click **Sign In/Register**.
3. Enter the user ID and password provided by Oracle Support, or create a new account.
4. On the Terms & Restrictions screen, select the boxes to indicate your acceptance of the License Agreement and Export Restrictions, and then click **Continue**.
5. Perform the following steps on the Media Pack Search screen:
   a. In the Select a Product Pack menu, select **Oracle StorageTek Products**.
   b. In the Platform menu, select **Linux x86-64**.
   c. Click **Go**.
6. Select the radio button for Oracle StorageTek Tape Analytics 2.0.x, and then click **Continue**.
7. Click **Download** for each of the two media pack ZIP files, and then save the ZIP files to a location containing at least 4 GB of free space.
8. Copy or move the ZIP files to any location on the target system (for example, /root).
9. Use an unzip tool to extract the STA TAR file from each ZIP file.

> **Note:** One of the ZIP files contains the STA release notes PDF. Read this document before installing and using STA.

10. To maintain correct file ownership/permissions, untar each TAR archive on the STA server using the following command:

```
# tar xvf STA_filename.tar
```

2.5 Install STA

You can install STA with the graphical installer (recommended) or console installer.

> **Note:** Before installing, see "Installation Checks" on page 2-1.

1. If using the graphical installer, set your DISPLAY environment variable. If you used **ssh -X** or **ssh -Y** to connect to the server, your DISPLAY variable should already be set.

```
# export DISPLAY=hostname:0.0
```

2. Change to the Disk1 directory:

```
# cd Disk1
```

3. As root, launch the installer with one of the following commands:
   - Graphical installer:

```
# ./install
```

   - Console installer:

```
# ./install -i console
```

4. Follow the wizard instructions to install STA, clicking **Next** (graphical installer) or pressing **`Enter`** (console installer) to advance the steps. Note that:
   - To go back to a previous step, click **Previous** (graphical installer) or type **`back`** (console installer). To cancel the installation, click **Cancel** (graphical installer) or type **`quit`** (console installer).
   - The installer will prompt you to create multiple STA user accounts and passwords. These are described in "User Accounts" on page 2-2.
   - The installer will prompt you to choose multiple ports for both internal and external STA server communication. These are described in "Port Configuration" on page 2-3. Specified port values will be checked to ensure they are not in use on the network.
   - The installer will prompt you for your company's domain name to configure Remote Diagnostics Agent (RDA). RDA is described in the "RDA Logging" chapter within the *StorageTek Tape Analytics Administration Guide*.
   - System changes are not implemented until you click **Install** (graphical installer) or press **`Enter`** (console installer) on the Pre-Installation Summary screen.
5. When the installation is complete and the STA installer has closed, ensure all services are running using the following command:

   ```
   # STA status all
   ```

   `STA` command usage is described in the "Server Administration" chapter within the *StorageTek Tape Analytics Administration Guide*.

3

Library Configuration Concepts

This chapter describes the concepts behind configuring libraries to send proper data to STA. Read this chapter before initiating the related configuration tasks in Chapter 4.

3.1 Library User Interfaces

The SL500, SL3000, and SL8500 libraries have a command line interface (CLI) and a graphical user interface, StorageTek Library Console (SL Console, standalone or web-based). The SL150 library exclusively uses a browser-based user interface.

For most CLI commands, the syntax is the same across the SL500, SL3000, and SL8500 library models. For the few commands where the syntax varies by library model, examples are provided. Most CLI examples use an SL500 library. If you are configuring an SL3000 or SL8500 library, the details returned by each command may vary slightly from what is shown.

CLI Usage Tips

- Use a terminal emulator, such as PuTTY, to establish an SSH (secure shell) connection to the library CLI.
- Enable logging so you can review your activity should you need to troubleshoot errors.
- SL500 library commands are case-sensitive.
- With some firmware versions, the CLI times out after six hours.
- To display help for any CLI command, type `help` plus the command name (for example, `help snmp`).

3.2 SNMP Configuration

Communication between the STA server and libraries is through the SNMP interface. The libraries send data to STA through SNMP traps, and STA retrieves library configuration data through SNMP "get" functions.

To establish communication between the STA server and the libraries, you perform configuration procedures on the libraries (as described in Chapter 4) and STA server (as described in Chapter 5).

For additional information about SNMP implementation on the libraries, see the *StorageTek Modular Libraries SNMP Reference Guide*.

Note: On a periodic basis, the MySQL Event Scheduler will purge processed SNMP records from the database to minimize database growth.

3.2.1 SNMP Communication

SNMP v3 is the recommended protocol for SNMP communications between STA and the libraries, and is also required for configuring Media Validation within STA (SL8500 only). Depending on your site requirements, however, you may choose to use v2c. Chapter 4 describes the recommended v3 configuration. See Appendix B, "Configuring SNMP v2c Mode," for information on configuring the v2c protocol.

Note: While STA uses the recommended SNMP v3 protocol to communicate with the library, the initial handshake between the library and STA server is through the v2c protocol.

The authentication, encryption, and message integrity features in SNMP v3 provide a secure mechanism for sending library data. To set up SNMP v3 communication on each library, you define the library as a v3 user and the STA server as a v3 trap recipient. In addition, you must specify authorization and privacy mechanisms and passwords. For STA, the authorization method is always SHA (Secure Hash Algorithm), and the privacy method is always DES (Data Encryption Standard).

3.2.2 Unique v3 User

STA supports only one SNMP v3 user. The same v3 user must be defined on all libraries monitored by a single STA server. Your libraries may already have one or more v3 users, and you can use one of these for STA communication. However, it is highly recommended that you set up a new, unique v3 user for this purpose.

3.2.3 SNMP Engine IDs

The SNMP v3 protocol requires each SNMP device to have a globally unique engine ID. Therefore, the STA server and the libraries each have their own unique engine IDs. In the case of SL8500 library complexes, each library in the complex also has its own SNMP agent, and therefore its own unique engine ID. The engine ID contains a maximum of 31 hexadecimal characters.

Traps use the sender's engine ID; therefore, you must specify the library engine ID when you define STA as the SNMP v3 trap recipient.

3.2.4 Duplicate Volume Serial Numbers

In the STA data store, media history is retained by volume serial number (volser). Because all history for a particular piece of media is tied to its volser, Oracle recommends that you avoid duplicate volsers. Volsers should be unique across all monitored libraries. Duplicate volsers will result in co-mingling of data for different pieces of media.

For more information on duplicate volsers, see the *StorageTek Tape Analytics Data Reference Guide*.

3.3 Dual TCP/IP and Redundant Electronics (SL3000 and SL8500 Only)

An SL3000 or SL8500 library can have one, two, or four IP addresses, depending on which features are activated. However, STA is capable of maintaining uninterrupted connections with up to two library IP addresses at a time. Therefore, on a given library, you can configure STA to support either Dual TCP/IP or Redundant Electronics (but not both). You must always specify a primary library IP address, but you can optionally specify a secondary IP address.

If STA is configured to support Dual TCP/IP, it will maintain a connection with the library in the event of a port failover. If STA is configured to support Redundant Electronics, it will maintain a connection with the library in the event of a controller card switch. After a Redundant Electronics switch completes, you must perform a connection test and data collection to verify the library connection and retrieve current library configuration data (see "SNMP Management Tasks" in the *STA Administration Guide*). See the library *User's Guide* for more information about these features.

> **Note:** For libraries with both features, Oracle recommends that you configure STA to support Redundant Electronics, as this feature is more critical to maintaining continuous library operations.

Table 3–1 summarizes the recommended library IP addresses to use when configuring the STA connection to the library.

Table 3–1 Recommended Library IP Addresses for STA Connection

Activated Features	Primary Library IP	Secondary Library IP
Neither	2B port	NA
Dual TCP/IP only	2B port	2A port, active card
Redundant Electronics only	active card 2B port	standby card 2B port
Both	active card 2B port	standby card 2B port

Additional Configuration Considerations

- To configure STA to support Dual TCP/IP on an SL3000 or SL8500 library, you may need to use policy routing. For more information, consult the SL3000 or SL8500 *Host Connectivity Guide*. If you need assistance with Dual TCP/IP configuration, contact Oracle Support.
- If a library has both Redundant Electronics and Dual TCP/IP, the STA server's subnet must be different from the subnet of the library port not configured for STA (STA GUI, "Define Library Connection Details" screen). Otherwise, the library may try to send information through those ports (unknown to STA) and it will be rejected by STA.
- Make sure your default gateway is the 2B interface.

3.4 Drive ADI Interface

LTO drives that support the Automation/Drive Interface (ADI) allow STA to provide high quality data (for example, drive performance and utilization), depending on configuration and firmware level. Drives that do not support ADI only provide basic data. ADI must be enabled on both the library and LTO drives. See the *STA Requirements Guide* for more information.

4

Library Configuration Process

This chapter describes the process for configuring libraries to send proper data to STA. Before configuring the libraries, you may need to prepare service requests for Oracle Support. See "Prepare Service Requests for Oracle Support" on page 2-viii.

> **Note:** This chapter assumes you will use the recommended SNMP v3 protocol for communications between the library and STA server. For more information, see "SNMP Communication" on page 3-2.

4.1 SNMP Configuration Worksheet

Before starting the library configuration process, you can fill out Table 4–1 to define the parameters you will use to configure SNMP on both the library and STA server.

Table 4–1 SNMP Configuration Parameters

Parameter	Description	Value
SNMP v2c community	SNMP v2c User Community string, commonly set to **public**. This string is required for the initial handshake between the library and STA server, even when using the SNMP v3 protocol. Can only contain alphanumeric characters (a-z, A-Z, 0-9). Special characters are not allowed.	
SNMP v3 user name	The STA server listens for traps sent by this user. It is also the v3 recipient name used when creating trap recipients. Must be the same on all libraries.	
SNMP v3 user authorization password	Authorization password you assign to the SNMP v3 user. Must be at least eight characters in length, and cannot contain commas, semicolons, or equal signs.	
SNMP v3 user privacy password	Privacy password you assign to the SNMP v3 user. Must be at least eight characters in length, and cannot contain commas, semicolons, or equal signs.	

4.2 Library Configuration Script (Optional)

You can use the library configuration script to display library CLI commands. It will step you through the library configuration process, request data to be entered, and then display commands that can be copied and pasted into the library CLI. To execute the script, issue the following command within a terminal session on the STA server:

```
# sh /Oracle/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
```

Note: Be sure to read and understand the library configuration steps in this chapter before executing the script.

For additional information about the script and to see example usage, issue the following command:

```
# sh /Oracle/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh -? |
more
```

4.3 Library Configuration Overview

You must complete all tasks listed in Table 4–2 for your library model, in the presented order.

Caution: Before starting the library configuration process, review the information in the *STA Requirements Guide*.

Table 4–2 Tasks to Configure Libraries for STA

Task	SL150	SL500	SL3000	SL8500
Task 1, "Log In to the Library"	Yes	Yes	Yes	Yes
Task 2, "Verify the Library Firmware Version"	Yes	Yes	Yes	Yes
Task 3, "Retrieve the Library IP Address"	Yes	Yes	Yes	Yes
Task 4, "Verify the Drive Controller Card Version (SL3000 and SL8500 Only)"			Yes	Yes
Task 5, "Enable ADI on the Library (All Libraries Except SL150)"		Yes	Yes	Yes
Task 6, "Enable SNMP on the Library"	Yes	Yes	Yes	Yes
Task 7, "Ensure an SNMP v2c User"	Yes	Yes	Yes	Yes
Task 8, "Create an SNMP v3 User"	Yes	Yes	Yes	Yes
Task 9, "Retrieve the Library SNMP Engine ID (All Libraries Except SL150)"		Yes	Yes	Yes
Task 10, "Create an SNMP v3 Trap Recipient"	Yes	Yes	Yes	Yes
Task 11, "Set the SL500 Volume Label Format"		Yes		
Task 12, "Set the SL150 Volume Label Format and Drive Element Addressing Mode"	Yes			
Task 13, "Set the Drive Cleaning Warning (SL3000 and SL8500 Only)"			Yes	Yes
Task 14, "Ensure the Correct Library Complex ID (SL8500 Only)"				Yes

4.4 Library Configuration Tasks

For SL500, SL3000, and SL8500 libraries, many tasks allow you to choose which interface to use — CLI or SL Console. For SL150 libraries, you exclusively use the browser-based user interface.

Task 1 Log In to the Library

With the CLI (all libraries except SL150)

1. Establish an SSH connection to the library using the IP address or DNS alias.
2. Log in to the CLI using the **admin** username and password.

With the SL Console (all libraries except SL150)

1. Start the SL Console application.
2. Click the **About** button to display the current SL Console version and verify that it meets the library firmware minimum requirements.
3. Click **Close** to return to the Login screen.
4. Log in using the **admin** user name, password, and library IP address or DNS alias.

   For SL3000 and SL8500 libraries with the Redundant Electronics feature, you can only log in to the active controller.

With the SL150 User Interface

1. Browse to the hostname or IP address of the SL150 library.
2. Log in with your user ID and password. The user ID must have the role of administrator.

Task 2 Verify the Library Firmware Version

Use this procedure to verify that the library firmware meets or exceeds the minimum requirements stated in the *STA Requirements Guide*. If it does not, contact Oracle Support to upgrade the firmware. For SL8500 libraries, Oracle Support must record the network connection settings before performing a firmware upgrade, as these settings may need to be re-entered or updated after the upgrade.

With the CLI (all libraries except SL150)[1]

Execute the following command:

```
SL500> version print
Library Hardware Information
 Library Vendor: STK
...
 Firmware Version: xxxx (x.xx.xx)
```

> **Note:** If the screen displays **SYNTAX ERROR!!**, the library firmware is down-level. Contact Oracle Support to upgrade the firmware.

With the SL Console (All libraries except SL150)

1. From the menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **Properties** > **Library Controller**.

[1] Not applicable to SL3000 libraries below FRS 4.x.

The firmware version is displayed under the Code Version section.

With the SL150 User Interface

Select **Firmware** from the navigation menu on the left side of the interface.

The firmware version is displayed under the Library Firmware section. Alternately, you can click the **About** button in the lower-right corner of the screen to obtain the firmware version.

Task 3 Retrieve the Library IP Address

Use this procedure to retrieve and record the library IP address, which you will use to configure the connection with the library. For SL3000 or SL8500 libraries, choose the method that matches your configuration for Dual TCP/IP, Redundant Electronics, or neither feature. For more information, see "Dual TCP/IP and Redundant Electronics (SL3000 and SL8500 Only)" on page 3-3.

SL500 IP Address

1. From the SL Console menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **Properties** > **General**.

   The library IP address is listed under the Library Interface TCP/IP section.
4. Record the library IP address as the primary library IP address. (This address corresponds to the 1B port.)

SL3000 or SL8500 IP Addresses — Dual TCP/IP Support

1. From the SL Console menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **Properties** > **General**.

   The IP address information is displayed in the Host Interface TCP/IP 2B and Host Interface TCP/IP 2A sections.

   Note: If the library also includes the Redundant Electronics feature, the IP addresses displayed are for the active controller card only.

4. Record the primary IP address (2B section) and secondary IP address (2A section).

SL3000 or SL8500 IP Addresses — Redundant Electronics Support

1. From the SL Console menu, select **Tools** > **System Detail**.
2. In the left panel, select the **Redundant Electronics** folder.

   If this folder is not listed, the Redundant Electronics feature is not available on the library.
3. In the Device State field, verify that one library controller shows **Duplex: software ready, switch possible** (this is the active card) and the other shows **Standby: software ready** (this is the standby card).

   These statuses indicate that the controller cards are functioning normally. If you do not see these statuses, contact Oracle Support.
4. Expand the **Redundant Electronics** folder, and then select the active controller card.

5. Record the IP address of the 2B port.
6. Repeat Step 4 and Step 5 for the alternate (standby) controller card.

SL3000 or SL8500 IP Addresses — No Dual TCP/IP nor Redundant Electronics

1. From the SL Console menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **Properties** > **General**.

   The IP address information is displayed in the Host Interface TCP/IP 2B section. There is no IP address information in the 2A section.
4. Record the IP address as the primary library IP address.

SL150 IP Address

In the SL150 user interface, select **Configuration** from the navigation menu on the left side of the screen.

The library IP address is displayed in the **Settings** > **Network** > **Network Port 1 Settings** section. (The **Network Port 2 Settings** section is reserved for service use.)

> **Note:** The Configure IP*xx* field value must be **Static**. If it is not, click the **Configure** button, and then select **Configure Network Settings** to specify a static IP address.

Task 4 Verify the Drive Controller Card Version (SL3000 and SL8500 Only)

Use the SL Console[1] to verify that a high-memory drive controller (HBT) card is installed in the library. For more information, see the *STA Requirements Guide*. Contact Oracle Support if you do not have a high-memory HBT card.

1. From the menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **Properties** > **Drive Controller**.

   The screen displays details about the active drive controller (HBT) card.
4. Verify that High Memory HBT indicates **true**.
5. If you have an SL3000 (FRS 4.x) or an SL8500 (FRS 8.x) library with Redundant Electronics, expand the Redundant Electronics folder, and then select each HBT card (hbta, hbtb). Both should indicate **True** for High Memory HBT.

> **Note:** Both the active and standby HBT cards must be installed and communicating, and both must have high memory.

Task 5 Enable ADI on the Library (All Libraries Except SL150)

If your library contains LTO drives, use this procedure to ensure that the ADI drive interface is enabled on the library. For more information, see "Drive ADI Interface" on page 3-3.

For SL3000 or SL8500 Libraries

1. Use the following command to display the status of the ADI interface:

[1] For SL8500 FRS 8.x and SL3000 FRS 4.x, you can also use the CLI `config print` command to display HBT card information.

```
drive adiEnable print
```

2. If "Attributes Adi Status" is **true**, you can quit this task. If it is **false**, proceed to the next step.
3. Use the following command to enable the ADI interface.

```
drive adiEnable on
```

4. Reboot the library to activate the change.

For SL500 Libraries

1. Use the following command to display the status of the ADI interface:

```
enableADI print
```

2. If "enableADI set to" is **on**, you can quit this task. If it is set to **off**, proceed to the next step.
3. Use the following command to enable the ADI interface:

```
enableADI on
```

4. Reboot the library to activate the change.

Task 6 Enable SNMP on the Library

Use this procedure to enable SNMP on the library public port.

With the CLI

- For SL3000 and SL8500 libraries, enable SNMP on port 2B. If the library includes the Dual TCP/IP feature, this command also enables SNMP on port 2A.

```
snmp enable port2b
```

- For SL500 libraries, enable SNMP on port 1B.

```
snmp enable port1B
```

With the SL Console (SL500 only)

1. From the menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **SNMP** > **Port Control**.
4. Complete the Port Control section as follows:

   Port: Select **Public (1B)**.

   Command: Select **Enable**.

5. Click **Apply**.

With the SL150 User Interface

1. Select **SNMP** from the navigation menu on the left side of the interface.
2. If SNMP shows as disabled, select **Enable SNMP**.
3. In the confirmation window, click **OK**.

Task 7 Ensure an SNMP v2c User

A v2c user is required for the initial handshake between the library and STA server. It is also required if you intend to use v2c for STA communication. For more

information, see "SNMP Configuration" on page 3-1. Before starting the procedure, note the following:

- There must be only one v2c user on the library.
- The community string can only contain alphanumeric characters (a-z, A-Z, 0-9). Special characters are not allowed.
- An existing v2c user is commonly set to the **public** community, but may be defined in another community name.
- You should not remove an existing v2c **public** user without consulting Oracle Service. In some cases, a v2c **public** user is required for Oracle Service Delivery Platform (SDP).

With the CLI (All libraries except SL150)

1. Use the following command to determine whether a v2c user already exists:

   ```
   snmp listUsers
   ```

2. If a v2c user is already defined, as in the following example, you can quit this task. If not, proceed to the next step.

   ```
   SL500> snmp listUsers
    ...
    Attributes Community public
    Index 1
    Version v2c
    Object Snmp snmp
    ...
   ```

3. Use the following command to add the SNMP v2c user:

   snmp addUser version v2c community *community_name*

   Where *community_name* is **public**, or another name. For example:

   ```
   SL3000> snmp addUser version v2c community public
   ```

4. List the SNMP users again to verify that the v2c user has been added correctly.

   ```
   snmp listUsers
   ```

With the SL Console (SL500 only)

1. From the menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **SNMP** > **Add Users**.
4. If a v2c user already exists in the Users section, you can quit this task. If not, proceed to the next step.
5. To add the SNMP v2c user, complete the **Add Users** tab as follows:

   Version: Select **v2c**.

   Community: Specify a community string (for example, **public**).

6. Click **Apply**.

With the SL150 User Interface

By default, the SL150 ships without a v2c user defined. If you plan to use v2c for STA communications, create a v2c user as follows.

1. Select **SNMP** from the navigation menu on the left side of the interface.
2. Under the SNMP Users section (or tab), select **Add SNMP User**.
3. In the Add SNMP User screen, complete the information as follows:

   Version: Select **v2c**.

   Community Name: Specify a community string (for example, **public**).
4. Click **OK**.

Task 8 Create an SNMP v3 User

All SNMP traps and MIB (management information base) data are sent to the STA server through the v3 user. Make a note of the username and passwords you specify, as you will use this information later in the configuration process. Note the following:

- The authorization method must be **SHA** (Secure Hash Algorithm), and the privacy method must be **DES** (Data Encryption Standard).
- All libraries monitored by a single STA server must have the same v3 user name. You should create a new, unique user for this purpose.
- Authorization and privacy passwords must be at least eight characters in length, and cannot contain commas, semicolons, or equal signs.
- To avoid entry errors in the CLI, you can first type the command in a text file, and then copy and paste it into the CLI. For help with CLI commands, type `help snmp`.

With the CLI (All libraries except SL150)

1. Use the following command to create a v3 user:

   `snmp addUser version v3 name` *`name`* **`auth SHA authPass`** *`auth_password`* **`priv DES privPass`** *`priv_password`*

   name: SNMP v3 user name

   auth_password and *priv_password*: Authorization password and privacy password.

   Note: For SL3000 and SL8500 libraries, enclose all variables in single quotes (Example 4–1).

Example 4–1 Create SNMP v3 User on SL3000 or SL8500

```
SL3000> snmp addUser version v3 name 'STAsnmp' auth SHA authPass 'authpwd1' priv
DES privPass 'privpwd1'
```

Example 4–2 Create SNMP v3 User on SL500

```
SL500> snmp addUser version v3 name STAsnmp auth SHA authPass authpwd1 priv DES
privPass privpwd1
```

2. List the SNMP users to verify that the v3 user has been added correctly.

   `snmp listUsers`

With the SL Console (SL500 libraries only)

1. From the menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **SNMP** > **Add Users**.

4. Complete the **Add Users** tab as follows:

   Version: Select **v3**.

   UserName: The name of the SNMP v3 user.

   Auth: Select **SHA**.

   AuthPass: Specify an authorization password.

   Priv: Select **DES**.

   PrivPass: Specify a privacy password.

5. Click **Apply**.

With the SL150 User Interface

1. Select **SNMP** from the navigation menu on the left side of the interface.
2. Under the SNMP Users section (or tab), select **Add SNMP User**.
3. For Version, select **v3**, and then complete the information as follows:

   User Name: The name of the SNMP v3 user.

   Authentication Protocol: Select **SHA**.

   Authentication Passphrase: Specify an authorization password.

   Privacy Protocol: Select **DES**.

   Privacy Passphrase: Specify a privacy password.

4. Click **OK**.

Task 9 Retrieve the Library SNMP Engine ID (All Libraries Except SL150)

Use one of the following CLI commands to display the library's SNMP engine ID (for example, 0x81031f88804b7e542f49701753). Save the engine ID to a text file for use in later configuration tasks.

- For SL3000 and SL8500 libraries:

  ```
  snmp engineId print
  ```

- For SL500 libraries:

  ```
  snmp engineId
  ```

Task 10 Create an SNMP v3 Trap Recipient

Use this procedure to define the STA server as an authorized recipient of SNMP traps, and to define the traps that the library will send. Note the following:

- Separate trap levels with commas.
- To avoid duplicate records, do not define the STA server as a trap recipient in multiple instances. For example, do not create both a v3 and v2c trap recipient definition for the STA server.
- Trap level 13 (Test Trap) and 14 (Health Trap) are new for STA 2.0.x. Trap level 4 may not be supported by older library firmware versions; however, it can always be specified when creating a trap recipient.
- To avoid entry errors in the CLI, you can first type the command in a text file, and then copy and paste it into the CLI. For help with CLI commands, type `help snmp`.

With the CLI (All libraries except SL150)

1. Use the following command to create a v3 SNMP trap recipient:

   snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host *STA_server_IP* **version v3 name** *recipient_name* **auth SHA authPass** *auth_password* **priv DES privPass** *priv_password* **engineId** *library_engineID*

   STA_server_IP: IP address of the STA server.

   recipient_name: SNMP user name you created in Task 8.

   auth_password and *priv_password*: Authorization and privacy passwords you created in Task 8.

   library_engineID: Library engine ID you displayed in Task 9, including the 0x prefix.

   Note: For SL3000 and SL8500 libraries, enclose *recipient_name*, *auth_password*, and *priv_password* in single quotes (Example 4–3).

Example 4–3 Create SNMP v3 Trap Recipient on SL3000 or SL8500

```
SL3000> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3 name
'STAsnmp' auth SHA authPass 'authpwd1' priv DES privPass 'privpwd1' engineId
0x00abcdef000000000000000000
```

Example 4–4 Create SNMP v3 Trap Recipient on SL500

```
SL500> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3 name
STAsnmp auth SHA authPass authpwd1 priv DES privPass privpwd1 engineId
0x00abcdef000000000000000000
```

2. List the trap recipients, and verify the recipient has been added correctly.

   snmp listTrapRecipients

With the SL Console (SL500 libraries only)

1. From the menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **SNMP** > **Add Trap Recipients**.
4. Complete the Trap Recipients screen fields as follows:

   Host: The IP address of the STA server.

   TrapLevel: Comma-separated list of trap levels the library should send to STA: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100.

   Version: Select **v3**.

   TrapUserName: SNMP user name you created in Task 8.

   Auth: Select **SHA**.

   AuthPass: Authorization password you created in Task 8.

   Priv: Select **DES**.

   PrivPass: Privacy password you created in Task 8.

EngineID: Library engine ID you displayed in Task 9. Do not enter the 0x prefix.

5. Click **Apply**.

With the SL150 User Interface

1. Select **SNMP** from the navigation menu on the left side of the interface.
2. Under the SNMP Trap Recipients section (or tab), select **Add Trap Recipient**.
3. Complete the fields as follows:

   Host Address: IP address of the STA server.

   Trap Level: Comma-separated list of trap levels the library should send to STA: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100.

   Version: Select **v3**.

   Trap User Name: SNMP user name you created in Task 8.

   Authentication Protocol: Select **SHA**.

   Authentication Passphrase: Authorization password you created in Task 8.

   Privacy Protocol: Select **DES**.

   Privacy Passphrase: Privacy password you created in Task 8.

   Engine ID: This field will auto-populate. Do not modify the value.
4. Click **OK**.

Task 11 Set the SL500 Volume Label Format

Use the following CLI commands to ensure that volume serial numbers (volsers) are formatted correctly in SNMP data sent to the STA server. Before starting this procedure, see "Volume Label Formatting Requirements (SL500 and SL150 Only)" in the *STA Requirements Guide*.

> **Note:** Oracle recommends that you quiesce all activity to the library before changing these parameters. Tape applications and/or hosts may require configuration changes after changing these parameters.

1. Display the current setting of the orientlabel flag.

```
SL500> orientlabel print
Host: (left8) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

2. “Host” must be set to “left6”. To do so, use the following command:

```
SL500> orientlabel host left6
New settings were accepted...Setting are now in effect.
```

3. Display the setting again to verify that it was updated correctly.

```
SL500> orientlabel print
Host: (left6) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

4. Display the current setting of the STA config flag.

```
SL500> staConfig print
STA mode is disabled
```

5. STA mode must be enabled. To enable the flag, use the following command:

```
SL500> staConfig on
```

6. Display the flag setting again to verify that it was updated correctly.

```
SL500> staConfig print
STA mode is enabled
```

Task 12 Set the SL150 Volume Label Format and Drive Element Addressing Mode

Use this procedure to ensure that volume serial numbers (volsers) are formatted correctly in SNMP data sent to the STA server, and to set the Drive Element Addressing Mode[1] so that empty drive bays are included in the data sent to STA. Before starting this procedure, see "Volume Label Formatting Requirements (SL500 and SL150 Only)" in the *STA Requirements Guide*.

> **Note:** Oracle recommends that you quiesce all activity to the library before changing these parameters. Tape applications and/or hosts may require configuration changes after changing these parameters.

1. Select **Configuration** from the navigation menu on the left side of the SL150 browser interface.
2. Select the **Configure** button.
3. In the Configuration Wizard window, select the **Configure Library Settings** check box, and then click **Next**.
4. Set the following parameters accordingly:
   - Drive Element Addressing Mode: **Address All Drive Slots (Recommended)**
   - Library Volume Label Format: **Trim last two characters (Default)**

   > **Note:** After changing the Drive Element Addressing Mode, you should wait at least 10 minutes before configuring SNMP in STA (see Chapter 5).

5. Click **Next**.
6. On the Summary of Configuration Changes screen, select the **Accept all changes** check box, and then click **Apply**.
7. In the Apply Configuration Changes screen, select the **Set the Library back Online after applying the changes** check box, and then click **OK**.
8. When you see **All configuration changes have been applied successfully**, click **Close**.

Task 13 Set the Drive Cleaning Warning (SL3000 and SL8500 Only)

Use this optional CLI procedure to check the current setting of the drive cleaning warning flag on the library and change it if necessary. The drive cleaning warning flag

[1] Only applicable to SL150 firmware 2.xx and above.

indicates whether a drive warning should be issued whenever a drive needs cleaning. This flag is set at the library level, so the same setting applies to all drives in a library.

- When the flag is set to “on”, each drive will show a warning health status whenever it needs cleaning. This will also cause the top-level health status of the library to be degraded in the STA monitor.
- When the flag is set to “off”, each drive’s status will not be affected by the need for cleaning. Therefore, the library top-level status in STA will not be degraded.

If you have a large number of drives in the library, you may want to set this flag to “off” so that the library top-level condition is not degraded whenever one of them needs cleaning.

1. Use the following command to display the current setting of the drive cleaning warning flag:

```
SL3000> cleaning driveWarning get
 ...
 Object Drive Cleaning Warning true
 ...
```

2. If you want to set the flag to “false” (off), use the following command:

```
cleaning driveWarning set off
```

Task 14 Ensure the Correct Library Complex ID (SL8500 Only)

Use this procedure to ensure the correct library complex ID information for each SL8500 library. Before starting this procedure, see "Complex ID Requirements (SL8500 Only)" in the *STA Requirements Guide*.

1. For each SL8500 library that will be monitored by STA, use the following command to display the complex ID currently assigned:

```
SL8500> config complexId print
 ...
 Complex Id 3
 ...
```

2. Verify that each standalone library and each library complex has a unique complex ID, and that all libraries in each library complex share the same complex ID.

   If you need to change the complex ID of a standalone library, continue this procedure.

   Caution: If you need to change the complex ID of a library in a library complex, contact Oracle Support. Do not continue with this procedure.

3. Place the library offline, and then wait for all transactions to complete.
4. Use the following command to change the complex ID of a standalone library, where *complex_ID* is a number, 1–127:

```
config complexId set complex_ID
```

Example 4–5 Change standalone SL8500 complex ID

```
SL8500> config complexId set 5
 ...
 Complex Id 5
```

```
Success true
Done
...
Note: TCP/IP stack reset may take a few seconds
after command completion.
```

Note: All TCP/IP connections are terminated when executing this command. You may have to log back in to the library.

5

Configuring SNMP in STA

After the libraries have been configured to send data to STA (as described in Chapter 4), use the following procedure to configure STA to receive data from the libraries.

5.1 STA Configuration Overview

To configure STA to receive SNMP data from the libraries, complete all the tasks in Table 5–1 in numerical order.

> **Note:** To minimize library disruption, perform Task 4 for all libraries before proceeding to Task 5. Then, perform Task 5 for all libraries before proceeding to Task 6.

Table 5–1 Tasks to Configure SNMP in STA

Task 1, "Verify SNMP Communications With the Library"
Task 2, "Log In to the STA User Interface"
Task 3, "Configure SNMP Client Settings for STA"
Task 4, "Configure SNMP Connections With the Library"
Task 5, "Verify the Library is Operational"
Task 6, "Test the SNMP Connection to the Library"
Task 7, "Get the Latest Configuration Data From the Library"

5.2 STA Configuration Tasks

Task 1 Verify SNMP Communications With the Library

This procedure verifies that UDP ports 161 and 162 have been enabled on all network nodes between the STA server and the library. It cannot validate that a v3 trap recipient has been specified correctly.

1. Establish a terminal session with the STA server, and log in as root.
2. At the command prompt, use the following command to test the SNMP v3 connection:

```
snmpget -v3 -u SNMP_user -a SHA -A auth_password -x DES -X priv_password -l
authPriv library_IP_addr 1.3.6.1.4.1.1211.1.15.3.1.0
```

- *SNMP_user*: The SNMP user you created in "Create an SNMP v3 User" on page 4-8.
- *auth_password*: The authorization password you assigned in "Create an SNMP v3 User" on page 4-8.
- *priv_password*: The privacy password you assigned in "Create an SNMP v3 User" on page 4-8.
- *library_IP_addr*: The IP address of the public port on the library, as follows:
  - For SL150 libraries, this is Network Port 1.
  - For SL500 libraries, this is port 1B.
  - For SL3000 and SL8500 libraries, there may be multiple ports to test, depending on whether Dual TCP/IP and/or Redundant Electronics are activated on the library. If there are multiple ports, run this command for each IP address.
- **1.3.6.1.4.1.1211.1.15.3.1.0**: The SNMP object identifier (OID) for the library, which is the same for all library models.

3. If the command output displays the library model (Example 5–1), the test is successful. If unsuccessful (Example 5–2), you may need to troubleshoot packet routing between the library and STA server. Contact your network administrator or Oracle Support.

Example 5–1 Successful snmpget Command

```
# snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1 -l authPriv
192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0
SNMPv2-SMI::enterprises.1211.1.15.3.1.0 =STRING: "SL8500"
```

Example 5–2 Unsuccessful snmpget Commands

```
# snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1 -l authPriv
192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0
Timeout: No Response from 192.0.2.20.

# snmpget -v3 -u WrongUsr -a SHA -A authpwd1 -x DES -X WrongPwd -l authPriv
192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0
snmpget: Authentication failure (incorrect password, community or key)
```

Task 2 Log In to the STA User Interface

1. Go to the STA GUI login screen using the HTTP (default is 7021) or HTTPS (default is 7022) port number you selected during STA installation. "STA" must be uppercase.

   http(s)://*yourHostName*:*PortNumber*/STA/

2. Log in using the STA GUI Login username and password.

Task 3 Configure SNMP Client Settings for STA

Use this procedure to configure STA to receive SNMP data from one or more libraries. You need to create one client entry for your site.

1. In the navigation menu, select **Setup & Administration** > **Configuration** > **SNMP Connections**.

2. In the Client Attributes table, select the empty table row. In the toolbar, click **Edit**.

3. Complete the Define SNMP Client Settings dialog box.

> **Note:** Even if STA will only be monitoring libraries configured for v2c communication, you must fill out all fields, including those applicable to v3. No fields may be left blank. See "SNMP Communication" on page 3-2.

   - **STA SNMP Connection Username (Auth)**: The SNMP v3 user name you created in "Create an SNMP v3 User" on page 4-8.
   - **Enter STA SNMP Connection Password (Auth)**: The connection authorization password you created in "Create an SNMP v3 User" on page 4-8.
   - **Enter Privacy Encryption Password (Privacy)**: The privacy encryption password you created in "Create an SNMP v3 User" on page 4-8.
   - **User Community**: Required for the initial handshake with the library, or if v2c will be used for STA communication. The default setting is **public**, but can be changed to match what is specified on the library. For more information, see "Ensure an SNMP v2c User" on page 4-6.
   - **Trap Community**: Only used if v2c will be used for communication with the library. When using v3, leave this set to the default, **public**. If using v2c for communication with the library, it can be changed to what is specified on the library.

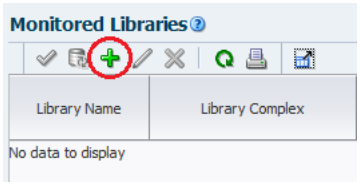
4. Click **Save**.

   A message reminds you that a library connection test is required. You will perform this test later in the process.

Task 4 Configure SNMP Connections With the Library

Use this procedure to configure SNMP connections between STA and a library. Perform this procedure for each library before proceeding to Task 5.

1. In the navigation menu, select **Setup & Administration** > **Configuration** > **SNMP Connections**.
2. In the Monitored Libraries toolbar, click **Add**.



3. Complete the Define Library Connection Details dialog box.

Note: For libraries with Dual TCP/IP or Redundant Electronics, see "Dual TCP/IP and Redundant Electronics (SL3000 and SL8500 Only)" on page 3-3 to determine which IP addresses to use.

- **Library Name**: This name will be used to identify the library throughout the STA user interface screens (for example, the library host name).
- **Library Primary IP Address**: The IP address of the primary public port on the library that you recorded in "Retrieve the Library IP Address" on page 4-4.
- **Library Secondary IP Address**: For SL500 and SL150 libraries, leave this field blank. For SL3000 and SL8500 libraries, enter the secondary IP address you recorded in "Retrieve the Library IP Address" on page 4-4.
- **STA IP Address**: Select the IP address of the STA server.
- **Library Engine ID**: Leave this field blank. This is the unique SNMP engine ID of the library automatically provided when the initial connection between STA and the library is made.
- **Automated Daily Data Refresh**: The time of day STA collects the latest configuration data from the library. The data will be collected automatically every 24 hours at this time. You should choose a time when there is typically lighter library usage. The default is 00:00 (12:00 am). Use 24-hour time format.

Caution: If you leave this field blank, scheduled automatic library data collections will be disabled. This will cause your STA library configuration data to become out of sync with the library.

- **Library Time Zone**: The library's local time zone.

4. Click **Save**.

   A message reminds you that a library connection test is required. You will perform this test later in the process.

5. Repeat this task for additional libraries.

Task 5 Verify the Library is Operational

Use this procedure to verify that a library is fully initialized and operational. If a library is not fully initialized, subsequent configuration steps will fail. Perform this procedure for each library before proceeding to Task 6.

SL500 Libraries

1. Log in to the library with the SL Console.
2. From the menu, select **Tools** > **System Detail**.
3. In the left panel, select **Library**.
4. In the right panel, select Status.
5. Verify the library Operational State indicates **Operational**.

SL3000 and SL8500 Libraries

1. Log in to the library with the SL Console.
2. From the menu, select **Tools** > **System Detail**.

3. In the left panel, select **Library**.
4. In the right panel, select **Status** > **General**.
5. Verify the Device State indicates “Ready”.

SL150 Libraries

1. Log in to the browser-based user interface.
2. At the top of the screen, verify that Health indicates **Operational**.

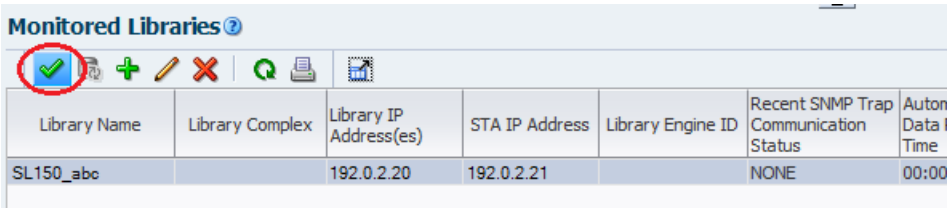
Task 6 Test the SNMP Connection to the Library

Use this procedure to test the SNMP connection between STA and each library. You should use this procedure whenever you add or modify STA or library SNMP information. Only one library connection can be tested at a time.

> **Note:** Because performing a connection test can cause a momentary loss of incoming packets, you should only do so when necessary.

1. In the STA navigation menu, select **Setup & Administration** > **Configuration** > **SNMP Connections**.
2. In the Monitored Libraries table, select a library, and then click **Check / Test Connection**.

   Test results for MIB Walk Channel, Trap Channel, and Media Validation[1] Support will appear momentarily. To troubleshoot a test[2], see "Troubleshooting Connection Tests and Data Collections" on page C-1.



3. Click **OK**. The Monitored Libraries table is updated, as follows:
   - The Library Complex field is blank, and will be updated in the next task.
   - The Library Engine ID field is populated. (A mismatch between the library engine ID shown here and the library engine ID specified when creating a trap recipient on the library does not affect the connection test.)
   - The Recent SNMP Trap Communication Status field indicates **NONE**.
   - The Last Successful Connection and Last Connection Attempt fields indicate the date and time when the connection test was completed and initiated, respectively.
   - The Last Connection Status field indicates “SUCCESS”.
4. Repeat this task for additional libraries.

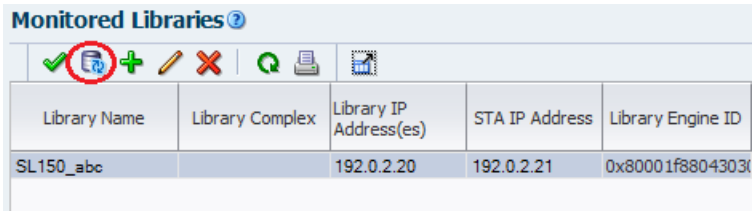
[1] See the *STA Requirements Guide* for more information.

[2] If a connection test or data collection fail due to a timeout, try performing these operations during a period of lower library activity.

Task 7 Get the Latest Configuration Data From the Library

After testing library connections in Task 6, you must use this procedure to manually initiate a data collection for each library. (Though STA performs a data collection automatically every 24 hours at the time you scheduled in Task 4, you must perform a manual data collection whenever you add SNMP connection information for a library.) Data collections may take several minutes to an hour, depending on library size.

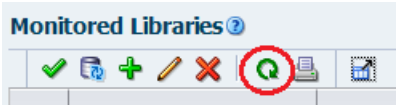
1. In the STA navigation menu, select **Setup & Administration** > **Configuration** > **SNMP Connections**.
2. Select a library in the Monitored Libraries table, and then click **Get latest data**.



Note: If you are completing this task for multiple libraries, you can initiate multiple "Get latest data requests" by selecting a library, clicking **Get latest data**, selecting another library, clicking **Get latest data**, and so on.

3. Click **OK** to dismiss the message box. In the Monitored Libraries table, Last Connection Status will update as follows:
   - **IN PROGRESS**: The data collection process is underway.
   - **SUCCESS**: The data collection was successful. STA starts receiving exchange data from the library.
   - **FAILED**: The data collection was not successful[2]. If possible, STA will provide information in the Last Connection Failure Detail field. (You may need to extend the column width to see the entire value.) See Appendix C, "Configuration Troubleshooting".

Note: The status is updated every four minutes, and the default screen refresh interval is 480 seconds. However, you can click the **Refresh Table** button to force a refresh of the table.



Note: Recent SNMP Trap Communication Status may occasionally indicate **MISSED HEARTBEAT**. This is normal.

6

Configuring Users and Email

This chapter describes configuring STA user roles and email recipients used for alerts and executive reports.

6.1 Configuring Users

During STA installation, you created an STA GUI Login account. This account is the primary STA administrator account. However, you can create additional user accounts with differing roles/permissions.

> **Note:** If you need to configure Open LDAP or IBM RACF user authentication, see Appendix A, "Configuring a SSP for STA"

6.1.1 User Roles

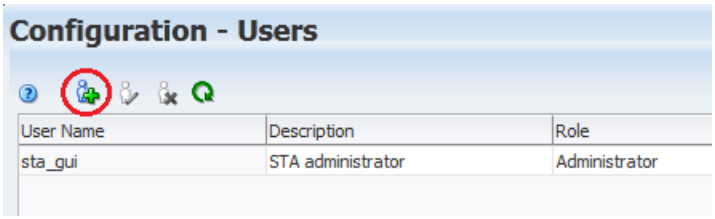
The following roles can be assigned to users:

- **Administrator**: Full access.
- **Operator**: Reduced access. An Operator has the same level of privileges as an Administrator, but cannot:
  - Create or edit Alerts policies or Executive Reports (but can run previously-defined reports)
  - Enable or disable Media Validation, nor create or edit Media Validation policies
  - Create or edit SNMP client attributes or library connections
  - Create, edit, or delete user accounts
  - Edit SMTP settings, nor test, create, edit, or delete email addresses
- **Viewer**: Limited/read-only access. Viewers cannot:
  - See the Setup & Administration tab in the STA navigation menu.

- Save templates (but can apply templates created by other users)
- Run Executive Reports (but can download reports already created)
- Save customizations (but can use existing customizations and filters)

6.1.2 Add a User

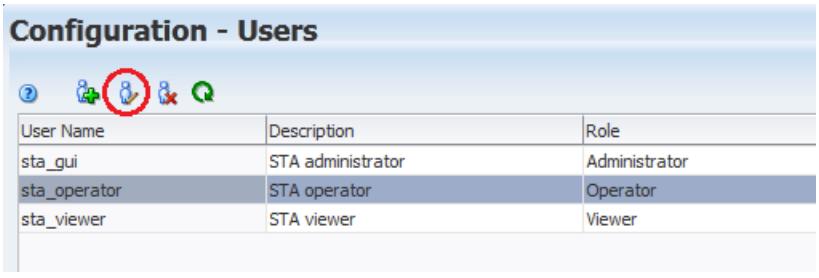
1. From the STA navigation menu, click **Setup & Administration** > **Configuration** > **Users**.
2. In the Configuration - Users section, click the **Create New User** button.



3. In the User Configuration window, complete the information as follows:
   - **User Name**: Enter the name of the user.
   - **Description**: Provide a description of the new user, if desired.
   - **Role**: Select Administrator, Operator, or Viewer.
   - **Enter Password**: Enter the login password for the new user. It must be at least eight characters long and contain a mix of letters and numbers.
   - **Verify Password**: Re-type the password.
4. Click **Save**.

6.1.3 Modify a User

1. From the STA navigation menu, click **Setup & Administration** > **Configuration** > **Users**.
2. In the Configuration - Users section, select a user name from the list, and then click the **Modify User** button.

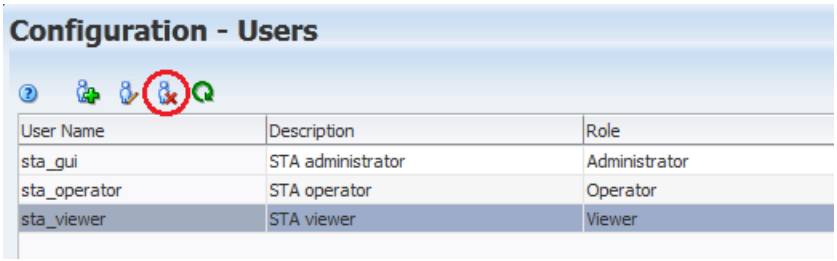


3. In the User Configuration window, modify the user Description, Role, or Password[1], and then click **Save**.

[1] You can also modify the current user's password in **Preferences** > **General**.

6.1.4 Delete a User

1. From the STA navigation menu, click **Setup & Administration** > **Configuration** > **Users**.
2. In the Configuration - Users section, select a user name from the list, and then click the **Delete User** button.



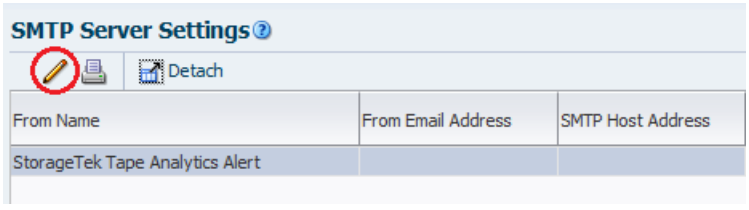
3. In the Delete User window, select to either make public or delete associated private templates or groups. Then, click **Delete**.

6.2 Configuring Email

STA's alert policies and Executive Reports both use configured email recipients for their respective communications. To set up alert policies and Executive Report policies, see the *STA User's Guide*.

6.2.1 Define SMTP Server Details

1. From the STA navigation menu, click **Setup & Administration** > **Configuration** > **Email**.
2. In the SMTP Server Settings table, select **StorageTek Tape Analytics Alert** (or a previously-specified name), and then click the **Edit Selected SMTP Server** icon located in the toolbar.



3. In the Define SMTP Server Details window, complete the information as follows:
   - **SMTP Host Address**: Enter the fully-qualified name of your SMTP server.

> **Note:** If the email server does not require authentication, you may need to specify **localhost** for the SMTP Host Address.

- **SMTP Port**: Enter the port number for outgoing mail transport.

  Typically, this is port 25, but check with your IT administrator to verify this is the port used at your site.

- **From Name**: Enter the name you want in the **From** line in your email. Text that identifies the STA server is recommended.

- **From Email Address**: Enter the email address from which the email is being sent.

  Since you cannot reply to this address, you may want to enter an address that indicates this, such as `DoNotReply@YourCompany.com`.

- **Enabled?**: Select the check box to enable the email server configuration.

- **Use Secure Connection Protocol**: Select the check box to use a secure connection protocol, and then select TLS or SSL.

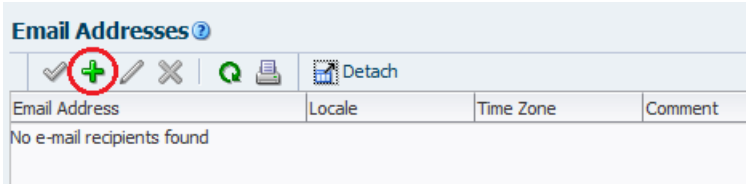
- **Requires Authentication**: Select the check box if the SMTP server requires authentication, and then enter the authentication username, password, and password verification.

4. Click **Save**.

6.2.2 Add an Email Address

Email notifications are sent to all configured email destinations. To add an email address:.

1. Click the **Add Email** icon located in the toolbar.



2. In the Define Email Details dialog box, complete the information as follows:

   - **Address**: Enter a destination for email notifications (for example, `yourname@your.company.com`).

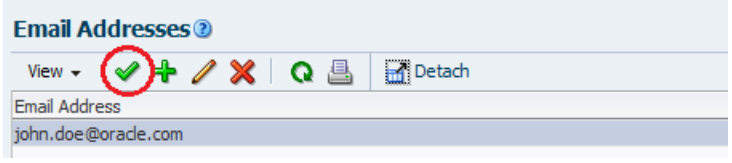
   - **Language-Locale**: Select the desired language-locale.

   - **Time Zone**: Select the recipient's time zone.

3. Click **Save**.

6.2.3 Test your SMTP and Email Address Setup

1. Select the email address, and then click the **Test SMTP and Email Address Setup** icon.



2. Go to the email client where you expect to receive the email.

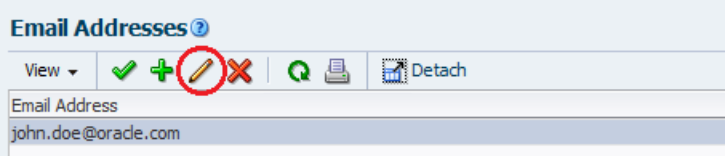
The test email should arrive momentarily. If it does not, check your STA configuration. If your configuration is correct, check with your system administrator.

Note: You can also check for email configuration problems in:

/Oracle/Middleware/user_projects/domains/TBI/servers/staEngine/logs/staEngine.log

6.2.4 Edit an Email Address

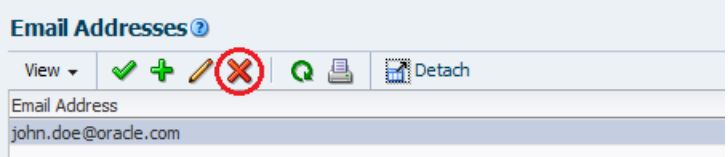
1. Select an email address from the table, and then click the **Edit Selected Email** icon.



2. In the Define Email Details dialog box, make any necessary changes, and then click **Save**.

6.2.5 Delete an Email Address

1. Select the email address(es) you want to delete.
2. Click the **Delete Selected Email(s)** icon located in the toolbar.



7

Configuring STA Services

Use these procedures to configure the STA Backup service and STA Resource Monitor service utilities located in /Oracle/StorageTek_Tape_Analytics/common/bin. For more information about these utilities, and to administer them after configuration, see the *STA Administration Guide*.

7.1 Update Linux PATH Setting (Optional)

Use this procedure to update the Linux PATH environment variable to include the location of the STA service utilities, `staservadm` and `staresmonadm`.

1. Open the profile for your user ID with a text editor. For example:

   ```
   # vi /root/.bash_profile
   ```

2. Add the above directory to the PATH definition. For example:

   ```
   # .bash_profile
   # User specific environment and startup programs

   PATH=$PATH:$HOME/bin
   PATH=$PATH:/Oracle/StorageTek_Tape_Analytics/common/bin

   export PATH
   ```

3. Save and exit the file.
4. Log out and log back in to Linux.
5. Display the setting for the PATH environment variable. The above STA directory should be displayed. For example:

   ```
   # echo $PATH
   /usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:
   /usr/sbin:/usr/bin:/root/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
   ```

7.2 Backup Configuration

You configure the STA Backup service with its administration utility, `staservadm`. To display a complete list of command options for the utility, type `staservadm -h`. For more information about the STA Backup service, see the *STA Administration Guide*.

Task 1 Review the staservadm Utility Preferences

Review Table 7–1 for descriptions of the available preference settings and to define your settings.

Table 7–1 STA Backup Service Administration Utility (staservadm) Attributes

Option	Attribute	Description	Default Value	Your Value
-S, --scp **-F, --ftp**	File transfer type	Method of file transfer used to copy the backup files from the STA server to the backup host. Options are SCP (recommended) or FTP.	SCP	
-T, --time	Full backup dump time	Time of day STA performs a full database backup dump. The dump is performed automatically every 24 hours at approximately this time. The actual time is sometime within "sleep interval" seconds after this time. Format is **hh:mm**, using 24-hour time.	00:00	
-i, --int	Sleep interval	Number of seconds the STA Services daemon waits before checking for new incremental backup files.	300	
-s, --server	Backup host name	IPv4 or IPv6 address or fully qualified DNS host name of the server host to which the STA server copies its backup files.	NA	
-u, --usr	Backup user ID	System user ID authorized to perform SCP file transfers to the backup host.	NA	
-p, --pwd	Backup password	Password assigned to the backup user.	NA	
-d, --dir	Backup directory	Directory on the backup host where the backup files will be copied.	NA	
-U, --dbusr	Database username	Database username authorized to perform a `mysqldump` command. You should specify the STA Database DBA Account username.	NA	
-P, --dbpwd	Database password	Password of the database username.	NA	

Task 2 Configure the Remote Backup Server

Use this procedure to configure a remote backup server (or equivalent) to receive the compressed backup files generated by the STA Backup service. Oracle recommends that you configure a remote backup server.

The required space is variable — the size should be a multiple of the size used for the STA_DB local backup, depending on the number of copies to be retained. Backup server storage should be mirrored or striped.

1. On the backup server, log in as the system root user.
2. Create a new group for the STA Backup user. For example:

   ```
   # groupadd -g 54321 stabckgr
   ```

   In this example, the group ID is "stabckgr", and the **-g** option is used to specify a numerical GID.
3. Create the STA Backup user. For example:

   ```
   # adduser stabck -c "STA database backup user" -m -d /home/stabck -g stabckgr
   ```

```
-s /bin/bash -u 98765
```

In this example, the user ID is "stabck", and the following options are used:

- **-c** – Comment.
- **-m** – Create a home directory for the user.
- **-d** – Full path of the home directory.
- **-g** – Assign the user to the specified group.
- **-s** – Assign the specified login shell to the user.
- **-u** – Assign the specified numerical UID to the user.

4. Assign a password to the STA Backup user. For example:

```
# passwd stabck
Changing password for user stabck.
New UNIX password: bckpwd1
Retype new UNIX password: bckpwd1
passwd: all authentication tokens updated successfully.
```

5. Create the directory where the STA backups will be copied. For example:

```
# cd /home/stabck
# pwd
/home/stabck
# mkdir -p STAbackups
# ls
STAbackups
```

In this example, the "STAbackups" directory is created in the STA Backup user's home directory, and the **-p** option is used to make parent directories as needed.

6. Display the user attributes to confirm that all information has been entered correctly. For example:

```
# cat /etc/passwd |grep sta
stabck:x:98765:54321:STA database backup user:/home/stabck:/bin/bash
```

7. Assign exclusive ownership and access rights for the directory to the STA Backups user and group. For example:

```
# chown -R stabck:stabckgr STAbackups
# chmod -R 700 STAbackups
# chmod 755 /home/stabck
```

In this example, the **-R** option is used to recursively assign the attributes to the directory and its files.

8. List the directory to confirm that all information has been entered correctly. For example:

```
# ls -la |grep STA
drw------- 2 stabck stabckgr 4096 Oct 19 14:20 STAbackups
```

Task 3 Configure the STA Backup Service

Use this procedure to configure the STA Backup service. You can designate a directory where the backup files will be copied. Oracle recommends that this directory be located on a remote backup server.

Your configuration settings take effect as soon as the service wakes from its current sleep interval and processes new settings or you manually restart the STA Services daemon ("Restart the STA Services Daemon (Optional)" on page 7-7).

1. On the STA server, log in as root.
2. Display the current STA Backup Service settings using the `staservadm -Q` command.

   This example shows that the service is not yet configured and is therefore not performing backups.

```
# ./staservadm -Q
Contacting daemon...connected.
Querying Preferences.
 Current STA Backup Service Settings:
   Configured            [no]
   File Transfer      -S [SCP]
   Full Backup        -T [00:00]
   Sleep Interval     -i [300 sec]
   Backup Hostname    -s []
   Backup Username    -u []
   Backup Password    -p []
   Backup Directory   -d []
   Database Username  -U []
   Database Password  -P []
```

3. Using Table 7–1 as a reference, set the attribute values with the `staservadm` command.

   You can submit the attributes in separate commands or combine them into one. For example:

```
# ./staservadm -S -T 11:00 -i 350 -s stabaksvr -u stabck -p bckpwd1 -d
/home/stabck/STAbackups -U sta_dba -P password1
```

   The utility sets each value included in your command and then displays all current settings. For example:

```
Contacting daemon...connected.
Setting File Transfer Type... SCP
Setting Sleep Interval..... 350
Setting Backup Hostname..... stabaksvr
Setting Backup Username..... stabck
Setting Backup Password..... *******
Setting Backup Directory..... /home/stabck/STAbackups
Setting Full Backup Time..... 11:00
Setting Database Username.... sta_dba
Setting Database Password.... *********
Done.
 Current STA Backup Service Settings:
   Configured            [yes]
   File Transfer      -S [SCP]
   Full Backup        -T [11:00]
   Sleep Interval     -i [350 sec]
   Backup Hostname    -s [stabaksvr]
   Backup Username    -u [stabck]
   Backup Password    -p [*******]
   Backup Directory   -d [/home/stabck/STAbackups]
   Database Username  -U [sta_dba]
   Database Password  -P [*********]
```

4. Review the command output to verify that the values have been set correctly.

7.3 Resource Monitor Configuration

You configure the STA Resource Monitor service with its administration utility, `staresmonadm`. To display a complete list of command options for the utility, type `staresmonadm -h` at the command line. For more information about STA Resource Monitor, including the reports it generates, see the *STA Administration Guide*.

Task 1 Review the staresmonadm Utility Preferences

Review the option descriptions in Table 7–2 and define your settings.

Table 7–2 STA Resource Monitor (staresmonadm) Attributes

Option	Attribute	Description	Default Value[1]	Your Value
-T, --time	Daily report time	Time of day STA sends a standard daily report. The report is sent automatically every 24 hours at approximately this time. The actual time is sometime within "sleep interval" seconds after this time. Format is **hh:mm**, using 24-hour time.	00:00	
-i, interval	Sleep interval	Number of seconds the STA Resource Monitor waits between scans.	300	
-n, --nag	Nag mode	Indicates how frequently STA alerts if any high watermarks are reached. If set to "on", STA sends alert emails every time the system is scanned. If set to "off", alerts are simply noted in the standard daily report.	Off	
-U, --dbusr	Database username	Database username authorized to perform queries against the "information_schema" tables and the MySQL server internal system global variables. You should specify either the STA Database DBA Account username or STA Database Root Account username (`root`).	NA	
-P, --dbpwd	Database password	The password assigned to the database username.	NA	
-t, --tblsphwm	Database tablespace HWM	High watermark for the database tablespace, entered as a percentage of the maximum available.	-1	
-b, --backvolhwm	Local backup HWM	High watermark for the STA local backups volume (/dbbackup), entered as a percentage of the maximum possible.	-1	
-d, --dbvolhwm	Database disk volume HWM	High watermark for the STA database volume (/dbdata/mysql), entered as a percentage of the maximum available.	-1	
-l, --logvolhwm	Logging disk volume HWM	High watermark for the STA database logs (/var/log/tbi/), entered as a percentage of the maximum available.	-1	
-z, --rootvolhwm	Root volume HWM	High watermark for the root volume (/), entered as a percentage of the maximum available.	-1	
-x, --tmpvolhwm	Tmp volume HWM	High watermark for the temporary directory volume (/tmp), entered as a percentage of the maximum available.	-1	
-m, --memhwm	Physical memory (RAM) HWM	High watermark for the total system memory (except virtual memory), entered as a percentage of the maximum available.	-1	
-f, --from	Email from	Name or email address that appears in the "From" field of the standard daily report email.	StaResMon@local host	

Table 7–2 (Cont.) STA Resource Monitor (staresmonadm) Attributes

Option	Attribute	Description	Default Value[1]	Your Value
-r, --recips	Email recipients	Recipient email addresses, entered as a colon-delimited list.	NA	
-s, --subject	Email subject	Entry that appears in the "Subject" field of the standard daily report email, up to 128 characters. Use quotes if it contains spaces. A timestamp in yyyy-mm-dd hh:mm:ss form will be appended to your entry when the email is sent.	STA Resource Monitor Report	
-o, --outfile	Output data file	Full path of the comma-separated (.csv) output data file.	/var/log/tbi/db/staresmon.csv	

[1] Default value of -1 indicates the attribute has not been configured.

Task 2 Configure the STA Resource Monitor

Use this procedure to configure the STA Resource Monitor service. Your configuration settings take effect as soon as the service wakes from its current sleep interval and processes new settings or you manually restart the STA Services daemon ("Restart the STA Services Daemon (Optional)" on page 7-7).

1. On the STA server, log in as root.
2. Display the current STA Resource Monitor settings using the `staresmonadm -Q` command.

   This example shows the service is not yet configured and is therefore not performing scans.

```
# ./staresmonadm -Q
Contacting daemon...connected.
Querying Preferences.
 Current STA Resource Monitor Service Settings:
   Configured                        [no]
   Send Reports                   -T [00:00]
   Sleep Interval                 -i [300 sec]
   Alert Nagging                  -n [off]
   DB Username                    -U []
   DB Password                    -P []
   DB Tablespace hwm              -t [-1%]
   DB Backup hwm   (/dbbackup)    -b [-1%]
   DB Data hwm     (/dbdata)      -d [-1%]
   Log Volume hwm  (/var/log/tbi) -l [-1%]
   Root Volume hwm (/)            -z [-1%]
   Tmp Volume hwm  (/tmp)         -x [-1%]
   System Memory hwm              -m [-1%]
   Email 'From:'                  -f [StaResMon@localhost]
   Email 'To:'                    -r []
   Email 'Subject:'               -s [STA Resource Monitor Report]
   Output File                    -o [/var/log/tbi/db/staresmon.csv]
```

3. Using Table 7–2 as a reference, set the attribute values with the `staresmonadm` command.

   You can submit the attributes in separate commands or combine them into one. For example:

```
# ./staresmonadm -T 13:00 -i 600 -n on -U sta_dba -P password1 -t 65 -b 65 -d
65 -l 65 -z 70 -x 80 -m 75 -r john.doe@company.com
```

The utility sets each value included in your command and then displays all current settings. For example:

```
Contacting daemon...connected.
Setting DB Tablespace HWM..... 65
Setting DB Disk Volume HWM.... 65
Setting Logging Volume HWM.... 65
Setting Backup Volume HWM..... 65
Setting Root Volume HWM....... 70
Setting Temp Volume HWM....... 80
Setting System Memory HWM..... 75
Setting 'To:' addresses....... john.doe@company.com
Setting Send Time............. 13:00
Setting Sleep Interval........ 600
Setting Alert Nag Mode........ ON
Setting DB Username........... sta_dba
Setting DB Password........... *********
Done.
 Current STA Resource Monitor Service Settings:
   Configured                        [yes]
   Send Reports                   -T [13:00]
   Sleep Interval                 -i [600 sec]
   Alert Nagging                  -n [on]
   DB Username                    -U [sta_dba]
   DB Password                    -P [*********]
   DB Tablespace hwm              -t [65%]
   DB Backup hwm   (/dbbackup)    -b [65%]
   DB Data hwm     (/dbdata)      -d [65%]
   Log Volume hwm  (/var/log/tbi) -l [65%]
   Root Volume hwm (/)            -z [70%]
   Tmp Volume hwm  (/tmp)         -x [80%]
   System Memory hwm              -m [75%]
   Email 'From:'                  -f [StaResMon@localhost]
   Email 'To:'                    -r [john.doe@company.com]
   Email 'Subject:'               -s [STA Resource Monitor Report]
   Output File                    -o [/var/log/tbi/db/staresmon.csv]
```

4. Review the command output to verify that the values have been set correctly.

7.4 Restart the STA Services Daemon (Optional)

Use this procedure to restart the STA Services daemon, **staservd**.

This procedure is useful if you changed the configuration settings of the STA Backup or STA Resource Monitor services and you want the new settings to take effect immediately. If you do not use this procedure, the new settings will take effect as soon as the service wakes up from its sleep interval and processes them.

1. Stop the STA Services daemon.

   ```
   # STA stop staservd
   ```

2. Start the STA Services daemon.

   ```
   # STA start staservd
   ```

3. Display the status of the daemon to confirm that it is running.

   ```
   # STA status staservd
   ```

7.5 Verify Library Connectivity

When you have finished configuring the services, confirm that all configured libraries have completed their "Get latest data" requests (Last Connection Status should indicate **SUCCESS**, and STA should be receiving exchange data from the libraries).

For more information, see "Get the Latest Configuration Data From the Library" on page 5-6.

8

Configuring Certificates

Oracle supplies self-generated certificates to be used with HTTPS/SSL Ports. During installation, STA generates a certificate using the Java keytool and creates it on your server using your server hostname. You can optionally replace the Oracle certificate with your own approved certificate from a selected certificate authority (for example, VeriSign).

Note: The following procedures use Mozilla Firefox running on a Windows platform.

8.1 Establishing the Initial HTTPS/SSL Connection

1. Enter the HTTPS/SSL version of the URL for the STA application on the browser.

   https://your_localhost.com:port number/STA/

2. Select **I Understand the Risks**, and then **Add Exception**.
3. Click **View** on the **Add Security Certificate** screen.

   You then see the Certificate Viewer: *your_localhost* screen. The certificate is not shown as verified because it is not from a certificate authority.

   You can examine the certificate further on the **Certificate Viewer** screen by clicking the **Details** tab and selecting the **issuer** field. The variables you may see include:

   - CN = The hostname of the server that the STA application has been installed on. For example,

     ```
     Common Name (CN) your server name
     ```

   - OU = Tape Systems
   - O = Oracle America Inc
   - L = Redwood City
   - ST = California
   - C = USA

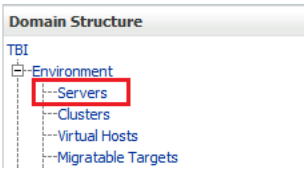
   The variable field CN is the server name that the certificate was generated on.

4. Click **Close** to return to the **Add Security Certificate** screen.
5. Select **Confirm Security Exception** on the **Add Security Certificate** screen, and you will be able to use HTTPS with the proper certificate.

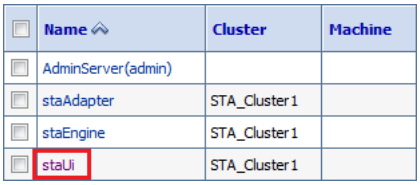
8.2 Reconfigure WebLogic to use a Different Security Certificate

1. Go to the WebLogic console login screen using the HTTP (default is 7001) or HTTPS (default is 7002) port number you selected during STA installation.

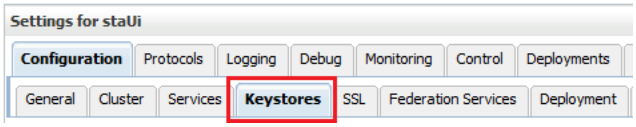
   http(s)://*yourHostName*:*PortNumber*/console/
2. Log in using the WebLogic Admin Console username and password you defined during STA installation.
3. Under Domain Structure > Environment, select **Servers**.



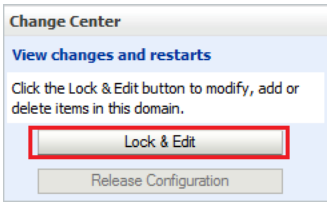
4. Under Servers, select **staUi** (select the name itself, not the check box).



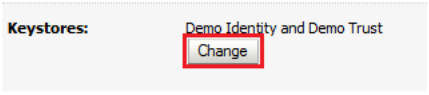
5. Select the **Keystores** tab.



6. Under Change Center (top left of screen), click **Lock & Edit**.



7. In the Keystores section, click **Change**.



8. In the Keystores drop-down menu, select **Custom Identity and Java Standard Trust**.
9. Click **Save**.
10. On the **Keystores** screen, enter:

a. **Custom Identity Keystore**: the path and file of the private key file.

b. **Custom Identity Keystore Type**: the keystore type. If configuring for RACF authentication, enter PKCS12.

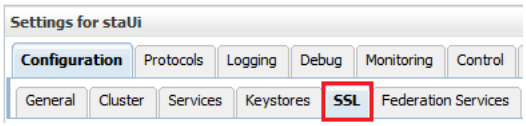
c. **Custom Identity Keystore Passphrase**: the password supplied by the MVS system administrator.

d. **Java Standard Trust Keystore Passphrase**: the new password for the Java Standard Trust Keystore file.

Caution: If you forget these passwords, you must re-install STA.

---

11. Click **Save**.
12. Select the **SSL** tab.



13. Enter the Private Key Alias and Private Key Passphrase supplied by the MVS system programmer.

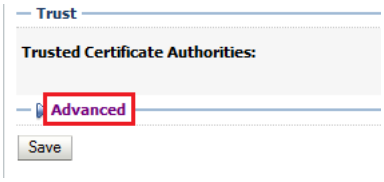
    To determine the Private Key Alias, use the `keytool` command. For example:

```
C:\Temp>keytool -list -keystore CLTBI.PKCS12DR.D080411 -storetype PKCS12
Enter keystore password: (password from the MVS sysadmin)
Keystore type: PKCS12
Keystore provider: SunJSSE

Your keystore contains 1 entry

tbiclient, Aug 17, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5): 9A:F7:D1:13:AE:9E:9C:47:55:83:75:3F:11:0C:BB:46
```

14. Click **Save**.
15. Select the **Advanced** link (bottom of screen).



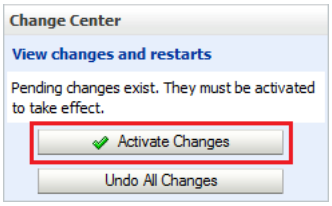
16. Modify the following information:

    a. Select the **Use Server Certs** check box.

    b. From the Two Way Client Cert Behavior list, select **Client Certs Requested But Not Enforced**.

    c. Select **Builtin SSL Validation Only** from both the Inbound Certification Validation and Outbound Certificate Validation lists.

17. Click **Save**.
18. Under the Change Center (top left of screen), click **Activate Changes**.



19. Log out of WebLogic.
20. Stop and restart STA with the `STA` command. For information on command usage, see the *STA Administration Guide*.

```
# STA stop all
# STA start all
```

8.3 Replace the Oracle Certificate

1. Enter the HTTPS/SSL version of the URL for the STA application on the browser.

   https://*your_localhost.com*:*port number*/STA/
2. Select **I Understand the Risks** on the **This Connection is Untrusted** screen.
3. Click **Add Exception**.
4. To specify a certificate for your organization, click **Get Certificate** on the **Add Security Certificate** screen and select the appropriate file.
5. Click **Confirm Security Exception**.

9 Upgrading STA

The process differs depending on the version from which you are upgrading (see Table 9–1). If you are deploying STA for the first time, perform a base/fresh installation as described earlier in this book.

Table 9–1 STA Upgrade Paths to Version 2.0.1 and Subsequent 2.0.x Versions

From Version	Instructions
1.0.0 **1.0.1** **1.0.2**	Go to "Upgrading STA 1.0.x to STA 2.0.x" on page 9-1 to upgrade any released STA 1.0.x version directly to 2.0.1 and subsequent 2.0.x versions.
2.0	Go to "Upgrading STA 2.0 to 2.0.x" on page 9-13 if you already have the initial release of STA 2.0 installed.

After upgrading, STA will process new data according to the new version's schema and analytic rules (historical data is not re-processed).

> **Note:** If you are simultaneously upgrading library firmware and STA, you may need to update the library engine ID and SNMP configuration. See "Managing SNMP Connections" within the *STA Administration Guide*.

9.1 Upgrading STA 1.0.x to STA 2.0.x

Upgrading STA 1.0.x to STA 2.0.x is a manual process consisting of multiple tasks and steps. Unlike the procedure to upgrade within major versions (for example, 1.0.1 to 1.0.2), the STA installer package cannot be used to automatically update the appropriate files.

9.1.1 Before Upgrading

Review the following before upgrading:

- You can upgrade only from the previous three STA 1.0 released versions: 1.0.0.99, 1.0.1.133, and 1.0.2.24.

To view the installed version, click **About** in the status bar in the lower-right corner of the STA screen.

- Review STA requirements — See the *STA Requirements Guide*.
- 4 GB (minimum) of /tmp space is required. For large databases, up to 32 GB may be required. The size of /tmp should be equal to or greater than the size of the uncompressed STA database.
- Move database backups to a separate server.

> **Caution:** Database backups created with the STA Backup Service will no longer be valid after the upgrade.

- WebLogic and MySQL credentials, port numbers, SNMP client attributes, and public templates with prefix "STA-" are *not* retained.

  Use the "Upgrade Worksheet" on page 9-2 to record STA 1.0.x settings. To use the same account usernames[1] and SNMP client attributes in STA 2.0.x, Task 1 provides instructions for obtaining this information.

> **Caution:** To keep any saved public templates with prefix "STA-", save them with new names before upgrading. After upgrading, other templates will show as public, owned by STA. Users can then load, assign as default, download, make modifications, save by a different name, and delete them.

- Ensure that STA 1.0.x is configured and operating properly.

  In the Monitored Libraries table, make sure that each library has had recent, successful communication with the STA server.
- STA 2.0.x consists of two large media pack ZIP files.

  You may want to start downloading the files now to a separate platform while completing the first few upgrade tasks (see "Download STA" on page 2-4).

9.1.2 Upgrade Worksheet

> **Caution:** See "Before Upgrading" on page 9-1 to review which STA 1.0.x credentials and settings are not retained.

Table 9–2 Required Information for STA 2.0.x Installation

Required Information	STA 1.0.x Values	STA 2.0.x Values[1]
WebLogic Admin Console login username		
WebLogic Admin Console login password		
STA GUI login username		
STA GUI login password		
STA database root account password[2]		

[1] In STA 2.0.x, additional application users are created within the STA UI, not WebLogic.

Table 9–2 (Cont.) Required Information for STA 2.0.x Installation

Required Information	STA 1.0.x Values	STA 2.0.x Values[1]
STA database application account username		
STA database application account password		
STA database reports account username		
STA database reports account password		
STA database DBA account username		
STA database DBA account password[2]		
WebLogic Admin Console login port, HTTP (default 7001)		
WebLogic Admin Console login port, HTTPS (default 7002)		
STA GUI login/staUi managed server port, HTTP (default 7021)		
STA GUI login/staUi managed server port, HTTPS (default 7022)		
staEngine managed server, HTTP (default = 7023)	NA	
staEngine managed server, HTTPS (default = 7024)	NA	
staAdapter managed server, HTTP (default = 7025)	NA	
staAdapter managed server, HTTPS (default = 7026)	NA	
Company domain name (for example, us.oracle.com)		

1 You can use existing STA 1.0.x values for STA 2.0.x or choose new values.

2 The database root or DBA account password is required for Task 2, "Dump the STA 1.0.x database".

Table 9–3 Required Information for STA 2.0.x Post-installation Configuration[1]

Required Information	STA 1.0.x Values	STA 2.0.x Values
SNMP v3 Username		
SNMP v3 Authorization Password (Auth)		
SNMP v3 Privacy Encryption Password (Privacy)		
User Community		
Trap Community		
Additional WebLogic username(s) and password(s)		

1 SNMP values must match what is specified on the library.

9.1.3 Upgrade Overview

You can upgrade STA 1.0.x to 2.0.x using one of these two methods:

- **Single server method (Figure 9–1)**: STA 1.0.x is offline (not monitoring libraries) while the server is reconfigured for STA 2.0.x, increasing downtime. You complete all tasks in numerical order.
- **Two server method (Figure 9–2)**: STA 1.0.x is online (monitoring libraries) on one server while a separate server is configured for STA 2.0.x, reducing downtime. With this method, the tasks are *not* completed in numerical order. You *must* complete the tasks in the order shown. Task 7 is omitted.

Figure 9–1 Single Server Upgrade Task Overview

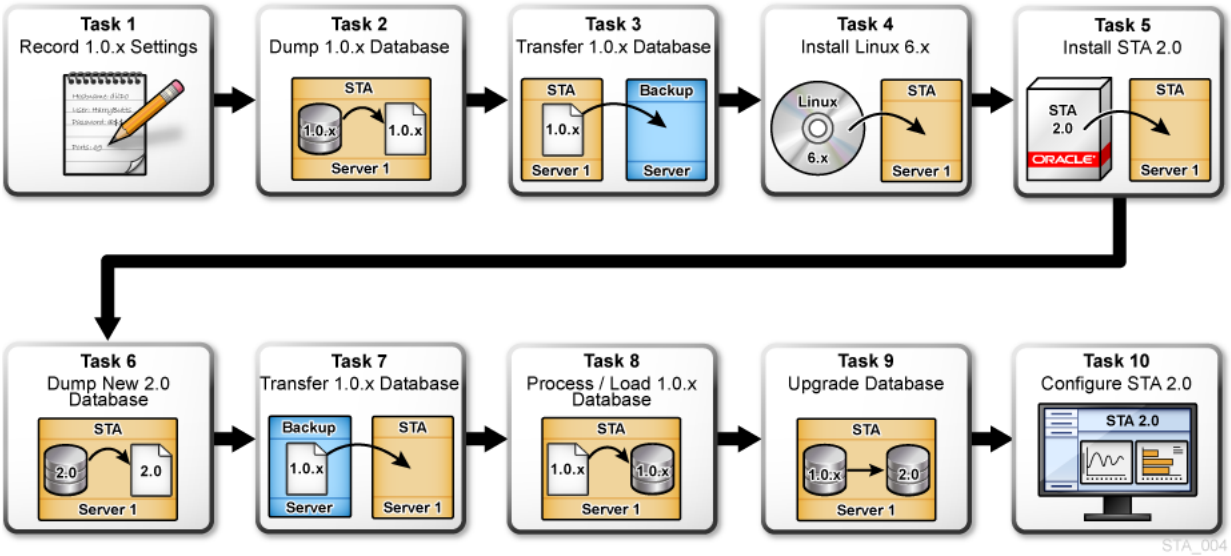
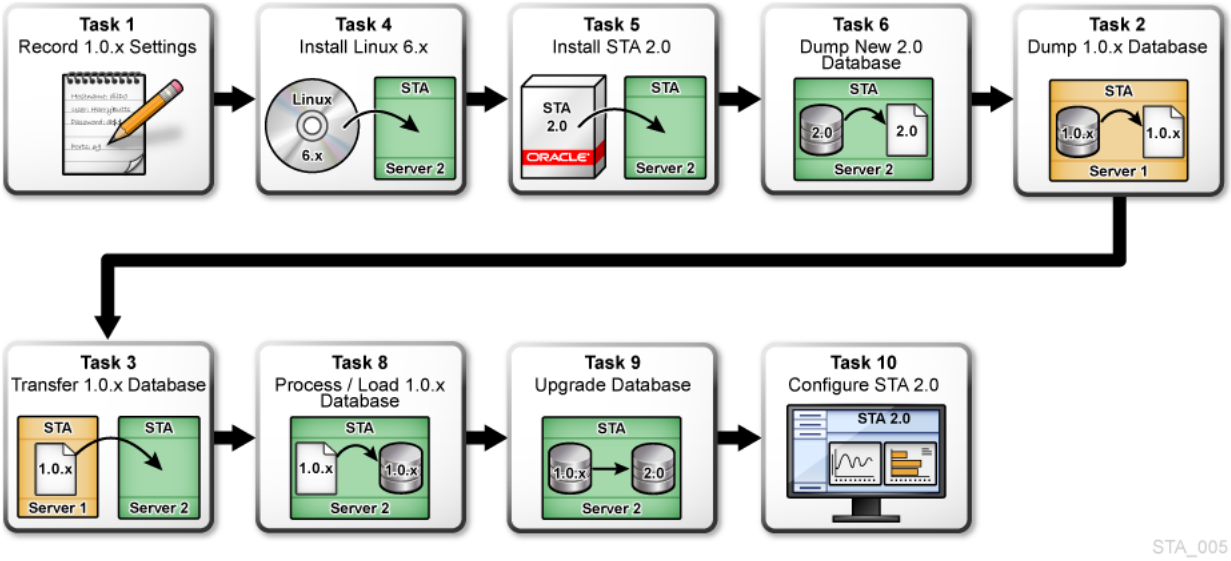


Figure 9–2 Two Server Upgrade Task Overview



9.1.4 Upgrade Process

- **Single server method (Figure 9–1)**: Complete all tasks in numerical order:

  Task 1, Task 2, Task 3, Task 4, Task 5, Task 6, Task 7, Task 8, Task 9, Task 10

- **Two server method (Figure 9–2)**: The tasks are *not* completed in numerical order. You *must* complete the tasks in the following order, omitting Task 7:

  Task 1, Task 4, Task 5, Task 6, Task 2, Task 3, Task 8, Task 9, Task 10

Caution: Only a Linux administrator and STA administrator should perform the upgrade. If the steps are not followed precisely as written in the specified order, data loss could result.

Task 1 (Optional) Record STA 1.0.x settings

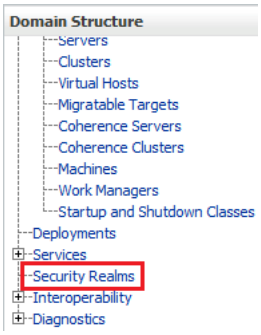
Use this procedure to obtain STA 1.0.x WebLogic usernames, MySQL database usernames, and SNMP client attributes. See "Before Upgrading" on page 9-1 for more information.

> **Note:** The passwords associated with the WebLogic, MySQL, and SNMP usernames are not retrievable.

1. To obtain a list of WebLogic users:
   a. Go to the WebLogic console login screen using the HTTP (default is 7001) or HTTPS (default is 7002) port number you selected during STA installation.

      http(s)://*yourHostName*:*PortNumber*/console/

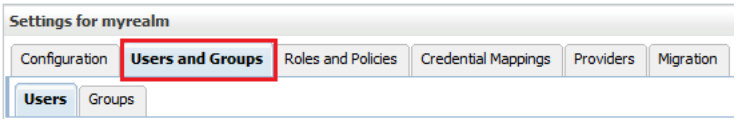
   b. Log in using the WebLogic Admin Console username and password.
   c. Under Domain Structure (left side of screen), click **Security Realms**.



   d. Under Realms, select **myrealm** (select the name itself, not the check box).

   e. Select the **Users and Groups** tab.

      The list of STA users appears within the Users table.



2. To obtain a list of MySQL database users:
   a. In a terminal session, log in to the STA 1.0.x server.
   b. Issue the following command and enter your MySQL root user password when prompted:

```
# mysql -uroot -p -e "select distinct(user) from user order by user ;"
mysql
Enter password: root-password
```

   c. Record the displayed list of STA database usernames. For example:

```
+--------+
| user   |
+--------+
```

```
| root   |
| staapp |
| stadba |
| starpt |
+--------+
```

3. To view SNMP client attributes:
   a. Go to the STA GUI login screen using the HTTP (default is 7021) or HTTPS (default is 7022) port number. "STA" must be uppercase.

      http(s)://*yourHostName*:*PortNumber*/STA/

   b. Log in using the STA GUI Login username and password.
   c. In the navigation menu, select **Settings** > **SNMP Connections**.

      The SNMP Username, User Community string, and Trap Community string are shown in the Client Attributes table.

Task 2 Dump the STA 1.0.x database

1. Open a terminal session on the STA 1.0.x server.
2. Issue the following command to stop all STA services:

   ```
   # STA stop
   ```

3. Start the MySQL service by issuing the following command:

   ```
   # service mysql start
   ```

4. Dump the database into a single file by issuing the following command:

   ```
   # /usr/bin/mysqldump -uroot -p --opt --routines --triggers --events
   --flush-logs --single-transaction --complete-insert --comments --dump-date
   --add-drop-database --databases stadb -v  > /desired_path_for_dumpfile/dump_
   file_name.sql
   Enter password: mysql_root_password
   ```

   Note: -v (optional, for verbose output) will echo the command progress. However, it can considerably slow down the dump process for large databases.

Example 9–1 STA 1.0.x database dump

In this example, the STA 1.0.x database is dumped into the **root** folder on the STA server with filename **20130711_dump.sql**.

```
# /usr/bin/mysqldump -uroot -p --opt --routines --triggers --events --flush-logs
--single-transaction --complete-insert --comments --dump-date --add-drop-database
--databases stadb -v  > /root/20130711_dump.sql
Enter password: mysql_root_password
...
-- Retrieving view structure for table v_library_complex_io...
...
-- Retrieving view structure for table v_library_summary_averages...
-- It's base table, skipped
...
-- Retrieving table structure for table v_mdv_status_codes...
-- It's a view, create dummy table for view
...
-- Disconnecting from localhost...
```

5. To reduce the dump file size by approximately 50%, gzip the file.

```
# cd /path_to_dump_file/
# gzip dump_file_name.sql
```

Task 3 Transfer the STA 1.0.x database

In this task, the compressed STA 1.0.x database dump file is either transferred to an off-platform backup server (single server method) or to the new STA 2.0.x server (two server method).

> **Caution:** When following the single server upgrade method, you must back up the STA database to another server. Do not back up the database to a filesystem on the existing STA server, as the Linux 6.x installation in Task 4 will destroy all data on the server.

1. Perform a checksum before transferring the file to the backup server.

```
# cksum dump_file_name.sql.gz
```

   The output will include a checksum value and byte count. Record the checksum value — you will use it to verify the file integrity after transferring the file to the backup server.

2. Transfer the file to the target server using a transfer utility such as SCP. The **-p** option preserves timestamp values.

```
# scp -p dump_file_name.sql.gz target_host:/path/
```

Example 9–2 STA 1.0.x database transfer to backup server (single server method)

In this example, the compressed database dump file **20130711_dump.sql.gz** is transferred with SCP to the **/root/dump** folder on backup host **backup1**.

```
# cd /root
# scp -p 20130711_dump.sql.gz backup1:/root/dump
```

Example 9–3 STA 1.0.x database transfer to new STA 2.0.x server (two server method)

In this example, the compressed database dump file **20130711_dump.sql.gz** is transferred with SCP to the **/root** folder on STA 2.0.x host **sta_new**.

```
# cd /root
# scp -p 20130711_dump.sql.gz sta_new:/root
```

3. On the target server, perform a checksum of the transferred file. Verify that the checksum value match.

```
# cd /path_to_dump_file/
# cksum dump_file_name.sql.gz
```

Task 4 Install Linux 6.x on the STA server

> **Caution:** If following the single server method, verify that the STA database was successfully backed up to another server. All data on the STA server will be destroyed in this task.

Because Linux 6.x is considered a major upgrade from Linux 5.x, an in-place upgrade is not supported by Linux — you cannot upgrade the OS while retaining existing Linux 5.x filesystems. Linux 6.x is installed fresh on the STA 1.0.x server.

To install and configure Linux 6.x, consult Chapter 1, "Installing Linux."

Task 5 Install STA 2.0.x on the STA server

1. Install STA as per Chapter 2, "Installing STA."
2. Log in to the STA user interface to ensure STA is working properly before performing the remaining upgrade tasks (see "Log In to the STA User Interface" on page 5-2).
3. Open a terminal session on the STA server.
4. Issue the following command to stop all STA 2.0.x services:

   ```
   # STA stop all
   ```

5. (Optional) If the STA 1.0.x server was configured to communicate with libraries with SNMP v2c, you will need to enable v2c mode on the STA 2.0.x server. Follow the procedure in Appendix B.3, "Enable SNMP v2c Mode for STA," but omit the final steps to stop and restart STA — this is unnecessary because you have already stopped STA and will restart it later in the upgrade process.

Task 6 Dump the newly-installed STA 2.0.x database

In case the upgrade fails, you will use a backup dump file to recover STA to a state in which you can configure STA to run as if it were freshly-installed with no data.

1. Start the MySQL service by issuing the following command:

   ```
   # STA start mysql
   ```

2. Issue the following command to create the backup file:

   ```
   # /usr/bin/mysqldump -uroot -p --opt --routines --triggers --events
   --flush-logs --single-transaction --complete-insert --comments --dump-date
   --add-drop-database --databases stadb -v > /dbbackup/STA_FRESH_INSTALL_
   BACKUP.sql
   Enter password: mysql_root_password
   ```

   Output will be similar to the following:

   ```
   ...
   -- Retrieving view structure for table v_mdv_request_states...
   -- Retrieving view structure for table version_info...
   ...
   -- Disconnecting from localhost...
   ```

   Note: If you see "Can't connect to local MySQL server," the MySQL server is not running. Make sure you have started MySQL (Step 1).

Task 7 Transfer the STA 1.0.x database to the STA 2.0.x server

Single server method only: You can use SCP to transfer the backed-up copy of the STA 1.0.x database to the STA 2.0.x server. The **-p** option preserves timestamp values.

1. Issue the following command:

   ```
   # scp -p backup_host:/path_to_dump_file/dump_file_name.sql.gz /local_path
   ```

Example 9–4 STA 1.0.x database transfer to STA 2.0.x server

In this example, the compressed database dump file **20130711_dump.sql.gz** is transferred with SCP from **/root/dump** on host **backup1** to the **/root** folder on the STA 2.0.x server.

```
# scp -p backup1:/root/dump/20130711_dump.sql.gz /root
```

2. Perform a checksum of the transferred file. Verify that the checksum value matches the value you received in Task 2.

```
# cd /path_to_dump_file/
# cksum dump_file_name.sql.gz
```

Task 8 Process and load the STA 1.0.x database

In this task, the compressed STA 1.0.x database is uncompressed and reinstated on the STA server.

1. Uncompress the backup file.

```
# gunzip dump_file_name.sql.gz
```

2. Perform the following steps to purge the STA database of obsolete data (for example, processed SNMP records and empty analytics records). This process will take approximately **30 seconds per gigabyte** of uncompressed database snapshot size to run.

> **Note:** A permanent record of `purgerecs` command activity is saved in the STA database. In STA 2.0.x, database purging also occurs automatically at runtime. On a periodic basis, the MySQL Event Scheduler will purge processed SNMP records from the database to minimize database growth.

   a. Change to the STA updates directory:

```
# cd /Oracle/StorageTek_Tape_Analytics/db/updates
```

   b. Issue the following command:

```
# ./purgerecs /path_to_dump_file/dump_file_name.sql /path_to_dump_
file/dump_file_name_PURGED.sql
```

> **Note:** For help with the `purgerecs` command, type the following:
>
> ```
> # ./purgerecs -h
> ```

Example 9–5 Purge obsolete data from STA 1.0.x database

In this example, the uncompressed MySQL dump file **20130711_dump.sql** in **/root** is purged with the `purgerecs` utility, with output directed to a new file called **20130711_dump_PURGED.sql** in **/root**. A progress dot will appear for each 200 records processed.

```
# cd /Oracle/StorageTek_Tape_Analytics/db/updates
# ./purgerecs /root/20130711_dump.sql /root/20130711_dump_PURGED.sql
.............................................
          STA v1.0.2, Schema 33.02
Processed 11,689 lines from '20130711_dump.sql':
---------------------------------------------
```

```
snmp_storage_cells........1,614,255
snmp_media................110,205
...
media_summaries...........254
transform_logs............0
================================================
Records Processed:........13,143,283
Records Purged:...........2,857,623
Records Remaining:........10,285,660
Elapsed Time:.............00:00:11
```

3. (Optional) Use the following command to determine the database file size and estimate the load process time. The load process will take up to **five minutes per gigabyte** of uncompressed database snapshot size to run.

   ```
   # ls -s -h dump_file_name_PURGED.sql
   ```

4. Load the STA 1.0.x database.

   ```
   # mysql -uroot -p -e "SET SESSION SQL_LOG_BIN=0; SOURCE /path_to_dump_
   file/dump_file_name_PURGED.sql;"
   Password: mysql_root_password
   ```

   If the command is successful, you will be returned to the command prompt once the process completes. Unless you specify the `-v` (verbose) option (not recommended), you will see no command output as the process runs.

   Command explanation:

   - **-p**: Prompts for the MySQL root password established during STA 2.0.x installation.
   - **-v**: Verbose output (optional). This will considerably slow down the load process.
   - **-e**: Execute the following quote-enclosed statement(s)
   - **SET SESSION SQL_LOG_BIN=0;**: This turns off unnecessary binary logging, which speeds up the load.
   - **SOURCE** */path_to_dump_file/dump_file_name*_**PURGED.sql**: Loads the dump file into the DB.

Task 9 Upgrade the database

The process will take approximately **two minutes per gigabyte** of uncompressed database snapshot size to run, depending on the STA 1.0.x version being upgraded.

1. Upgrade the STA 1.0.x database to the new STA 2.0.x schema by issuing the following commands:

   ```
   # cd /Oracle/StorageTek_Tape_Analytics/db/updates
   # ./upgradedb.sh
   DB Root Password: mysql_root_password
   ```

   Note: For security reasons, the password will not be echoed. For help with the `upgradedb.sh` command, type the following:

   ```
   # ./upgradedb.sh -h
   ```

   Example output:

```
+------------------------------------------------------------+
| STA DATABASE UPGRADE                                       |
| Upgrading DB schema from 49.00r0 to 50.00r0                |
| Started: 2014-01-14 01:21:47                               |
+------------------------------------------------------------+
STA database contains approximately 4,301 records.
installed version 49.00 is a valid upgrade candidate, proceeding...
...allow approximately two minutes per 1GB of file size...
```

When the process is complete, you will see a banner similar to the following:

```
+------------------------------------------------------------+
| Started.................2014-01-14 01:21:47                |
| Finished................2014-01-14 01:21:54                |
| Elapsed Time............00:00:07                           |
| Starting Version........49.00r0                            |
| Final Schema Version....50.00r0                            |
| Schema Release Date.....2014-01-08 15:16:17                |
| Records (approximate)...4,282                              |
+------------------------------------------------------------+
```

Note: If the upgrade fails, you may attempt Task 8, Step 4 through Task 9. If the upgrade fails again, the database is in an unknown, possibly damaged state. In that case, you should restore the database to its original, freshly-installed state, as follows:

1. Delete the damaged upgraded database.

   ```
   # mysql -uroot -p -e "drop database stadb;"
   ```

2. Load the fresh installation database dump file you created in Task 6.

   ```
   # cd /dbbackup
   # mysql -uroot -p -e < STA_FRESH_INSTALL_BACKUP.sql
   ```

3. After performing Task 9, configure STA as a new installation.

2. Start all STA services by issuing the following command.

   ```
   # STA start all
   ```

Caution: Do not start STA until the database upgrade process has completely finished in Step 1 of this task.

3. (Optional) If the upgrade is successful, delete the STA_FRESH_INSTALL_BACKUP.sql file to free up disk space on the /dbbackup volume.

Task 10 Configure STA 2.0.x

1. Proceed according to the upgrade method:

   - **Single server method**: If you changed the STA server's IP address during the upgrade process, re-add each library's trap recipient list to reflect the new IP address of the STA server. To re-add trap recipients, see "SNMP Management Tasks — Library" in the *STA Administration Guide*.
   - **Two server method**: Add the STA 2.0.x server as a new trap recipient to each library's SNMP configuration. See "Create an SNMP v3 Trap Recipient" on page 4-9 or "Create an SNMP v2c Trap Recipient" on page B-1.

> **Note:** STA 2.0.x supports two new trap levels, 13 (Test Trap) and 14 (Health Trap). If these levels have not previously been specified on each monitored library's trap recipient list, you will also need to re-add the trap recipient list with levels 13 and 14 included.

2. Log in to STA, as described in "Log In to the STA User Interface" on page 5-2.
3. Re-enter the SNMP client attributes, as described in "Configure SNMP Client Settings for STA" on page 5-2.
4. Update the connection details for each monitored library.
   a. In the navigation menu, select **Setup & Administration** > **Configuration** > **SNMP Connections**.
   b. In the Monitored Libraries section, select a library name, and then click the **Edit** button.
   c. Select the IP address of the STA 2.0.x server in the STA IP Address drop-down.
   d. Click **Save**.
   e. Repeat these steps for each monitored library in the list.
5. To ensure proper communications, test the connection to each configured library, as described in "Test the SNMP Connection to the Library" on page 5-5.

   Before testing a connection, make a note of the Last Successful Connection and Last Connection Attempt timestamps. Once you have performed a test, you can compare the timestamps to ensure the test is providing current information.
6. Get the latest data from each library, as described in "Get the Latest Configuration Data From the Library" on page 5-6.
7. Follow the procedures in "Configuring Users and Email" on page 6-1 to change or create STA users and configure (and test) email properties.

   If additional STA users (beyond the default Admin Console Login and STA GUI Login users) were recorded in Task 1, you can create these same users now and assign them roles as appropriate.

   > **Note:** While most of the email notification settings are retained when upgrading STA, you will need to re-enable SMTP communication and re-enter your email account password.

8. Configure (or re-configure) the remaining components of STA, as per the following chapters:
   - Chapter 7, "Configuring STA Services"
   - Chapter 8, "Configuring Certificates"
9. If you followed the two server method, you may now decommission the STA 1.0.x server.

   You may optionally remove the STA 1.0.x server as a trap recipient from each library's SNMP configuration. To delete trap recipients, see "SNMP Management Tasks — Library" in the *STA Administration Guide*.

9.2 Upgrading STA 2.0 to 2.0.x

Unlike the procedure to upgrade STA 1.0.x to 2.0.x, which is a manual process, upgrading STA 2.0 to 2.0.x uses the installer package to automatically update the database files. Therefore, do *not* uninstall STA before upgrading, as this will remove the STA database.

9.2.1 Before Upgrading

Review the following before upgrading:

- You can upgrade only from STA 2.0.0.83.

  To view the installed version, click **About** in the status bar in the lower-right corner of the STA screen.

- 4 GB (minimum) of /tmp space is required. For large databases, up to 32 GB may be required. The size of /tmp should be equal to or greater than the size of the uncompressed STA database.

- Oracle highly recommends you back up the STA database before upgrading.

  1. Open a terminal session on the STA server.
  2. Stop all STA services.

     ```
     # STA stop all
     ```

  3. Start MySQL.

     ```
     # STA start mysql
     ```

  4. Dump the STA database into a backup file.

     ```
     # /usr/bin/mysqldump -uroot -p --opt --routines --triggers --events
     --flush-logs --single-transaction --complete-insert --comments --dump-date
     --add-drop-database --databases stadb  > /desired_path_for_dumpfile/dump_
     file_name.sql
     Enter password: mysql_root_password
     ```

- Move database backups to a separate server.

  Caution: Database backups created with the STA Backup Service or `mysqldump` command are applicable only to the pre-upgrade STA version. To avoid data corruption, they should not be used for recovery in the new STA version. Retain these backups until you confirm the upgrade was successful and a new, full database backup is completed. To configure the STA Backup Service after upgrading, see Chapter 7, "Configuring STA Services".

- User-modified alerts with prefix "STA-" will be renamed with prefix "ZOLD_ STA-", and then new STA- alerts (possibly having the same name) will be installed.

  After upgrading, you should compare the active ZOLD_STA- rules to the new STA- rules and decide if the new rules are preferable.

9.2.2 Upgrade Worksheet

The STA installer will prompt you for the following information during the upgrade process. Gather this information and fill in Table 9–4.

> **Note:** Username, password, and port information should already be recorded in "User Accounts" on page 2-2 and "Port Configuration" on page 2-3.

Table 9–4 Required Information for Upgrading STA 2.0 to 2.0.x

Required Information	Value
WebLogic Admin Console login username	
WebLogic Admin Console login password	
WebLogic Admin Console port number (HTTP or HTTPS)	
STA Database (MySQL) Root Account password	

9.2.3 Upgrading STA

1. Remove the Disk1 and Disk2 folders from the target system. (These folders were created when STA was originally installed.) For example:

   ```
   # rm -rf Disk1
   # rm -rf Disk2
   ```

2. Download the latest version of STA. Follow the procedure in "Download STA" on page 2-4.
3. Upgrade STA. Follow the procedure in "Install STA" on page 2-5, except:
   - After launching the installer, you will need to click **OK** (graphical installer) or select the "Continue" option (console installer) to confirm you want to upgrade.
   - You will only be prompted for the information in Table 9–4.

   Depending on the size and type of data in the STA database, the upgrade process may take 20-30 minutes.
4. Restore the STA services daemon.

   If you previously configured the STA Backup Service, Resource Monitor Service, or both, perform the following steps. If you previously configured neither of these services, proceed to Step 7.

   a. Shut down the STA services daemon.

   ```
   # STA stop staservd
   ```

   b. Remove the existing wallet file and log files.

   ```
   # cd /Oracle/StorageTek_Tape_Analytics/common/conf
   # rm cwallet.sso cwallet.sso.old
   # cd /var/log/tbi/db/backups
   # rm *.log.*
   ```

   c. Restart the STA services daemon.

   ```
   # cd ~
   # STA start staservd
   ```

5. Restore the STA Backup Service.

   If you previously configured the STA Backup Service, perform the following steps to restore the username and password for this service. If you did not previously enable this service, proceed to Step 6.

   a. Show the current state of the STA Backup Service. For example:

   ```
   # staservadm -Q
   Contacting daemon...connected.
   Querying Preferences.
   Current STA Backup Service Settings:
   Configured            [yes]
   ...
   ```

   b. Restore the database credentials using the STA DBA account username and password you chose during STA installation.

   ```
   # staservadm -U dba_username -P
   Enter database password: dba_password
   Contacting daemon...connected.
   Setting Database Username.... dba_username
   Setting Database Password.... ********
   Done.
   ...
   ```

   c. Restore the login credentials for the remote backup server using the system login username and password you used to configure the STA backup server.

   ```
   # staservadm -u backup_server_username -p
   Enter backup password: backup_server_password
   Contacting daemon...connected.
   Setting Backup Username...... backup_server_username
   Setting Backup Password...... ********
   Done.
   ...
   ```

   d. Restart the STA services daemon.

   ```
   # cd ~
   # STA stop staservd
   # STA start staservd
   ```

   e. (Optional) Observe the STA services daemon log.

   ```
   # tail -f /var/log/tbi/db/backups/staservd.log.0
   ```

6. Restore the STA Resource Monitor Service.

   If you previously configured the STA Resource Monitor Service, perform the following steps to restore the username and password for this service. If you did not previously enable this service, proceed to Step 7.

   a. Show the current state of the STA Resource Monitor Service. For example:

   ```
   # staresmonadm -Q
   Contacting daemon...connected.
   Querying Preferences.
   Current STA Resource Monitor Service Settings:
   Configured                      [yes]
   ...
   ```

b. Restore the database credentials using the STA DBA account username and password you chose during STA installation.

```
# staresmonadm -U dba_username -P
Enter database password: dba_password
Contacting daemon...connected.
Setting DB Username.......... dba_username
Setting DB Password.......... ********
Done.
...
```

c. Restart the STA services daemon.

```
# cd ~
# STA stop staservd
# STA start staservd
```

d. (Optional) Observe the STA services daemon log.

```
# tail -f /var/log/tbi/db/backups/staservd.log.0
```

7. (Optional) Delete installer backup files.

During the upgrade process, the installer creates a .tar file that contains backup copies of the following directories:

- /Oracle/StorageTek_Tape_Analytics
- /Oracle/StorageTek_Tape_Analytics/install

After the upgrade is successful, you can delete this file. The file is located in /Oracle/StorageTek_Tape_Analytics/backup_*x.x.x.xx*, where *x.x.x.xx* is the previous STA version number.

10

Uninstalling and Reinstalling STA

This chapter details the uninstallation and reinstallation of STA.

> **Caution:** Oracle does not support downgrading STA to a prior version. Database data created with a newer version of STA will be lost when installing an older version of STA.

10.1 Uninstalling STA

You can uninstall STA with the graphical installer (recommended) or console installer. If you originally installed STA using the console mode, the uninstaller will only run in console mode.

If using the graphical uninstaller, set your DISPLAY environment variable before proceeding. If you used **ssh -X** or **ssh -Y** to connect to the server, your DISPLAY variable should already be set.

```
# export DISPLAY=hostname:0.0
```

> **Caution:** All STA database data will be removed. Perform a backup before uninstalling. The following directories are removed:
>
> - /Oracle/Middleware
> - /Oracle/StorageTek_Tape_Analytics
> - /var/log/tbi

1. Change to the STA install directory:

   ```
   # cd /Oracle/StorageTek_Tape_Analytics_install
   ```

2. Launch the uninstaller with one of the following commands:

   - Graphical uninstaller:

     ```
     # ./Uninstall_StorageTek_Tape_Analytics
     ```

   - Console uninstaller:

     ```
     # ./Uninstall_StorageTek_Tape_Analytics -i console
     ```

3. Follow the wizard instructions to uninstall STA, clicking **Uninstall** (graphical installer) or pressing **Enter** (console installer).

10.2 Reinstalling STA

You cannot use the STA installer package to reinstall/overwrite a current installation. Use this procedure to reinstall STA (for example, to repair a current installation).

1. Perform a manual log snapshot. See "Take an RDA Snapshot" in the "RDA Logging" chapter within the *STA Administration Guide*.
2. Stop all STA services:

   ```
   # STA stop all
   ```

3. Perform a database snapshot.
   a. Start the MySQL service by issuing the following command:

      ```
      # STA start mysql
      ```

   b. Issue the following command to create a backup file:

      ```
      # /usr/bin/mysqldump -uroot -p --opt --routines --triggers --events
      --flush-logs --single-transaction --complete-insert --comments --dump-date
      --add-drop-database --databases stadb -v > /dbbackup/backup_filename.sql
      Enter password: mysql_root_password
      ```

      Output will be similar to the following:

      ```
      ...
      -- Retrieving view structure for table v_mdv_request_states...
      -- Retrieving view structure for table version_info...
      ...
      -- Disconnecting from localhost...
      ```

      Note: If you see "Can't connect to local MySQL server," the MySQL server isn't running. Make sure you have started MySQL (Step a).

4. Move the log snapshot taken in Step 1 (located in /Oracle/Middleware/rda/snapshots) and database snapshot taken in Step 3 (located in /dbbackup) to another server, as all STA files will be removed in the next step. Back up other files as needed.
5. Uninstall STA as per "Uninstalling STA" on page 10-1.
6. Re-install STA as per Chapter 2, "Installing STA."
7. Stop all STA services:

   ```
   # STA stop all
   ```

8. Restore the database as per "Reload the Database" in the "Database Services Administration" chapter within the *STA Administration Guide*.
9. Start all STA services:

   ```
   # STA start all
   ```

10. Configure STA. Follow Task 10, "Configure STA 2.0.x" on page 9-11, Step 2 through Step 8.

A

Configuring a SSP for STA

You must authenticate users before they can be allowed access to STA. Local user creation and role assignment is handled within the STA application, and is described in "Configuring Users" on page 6-1. This chapter describes configuring an external security service provider (SSP) for STA: Open LDAP and IBM Resource Access Control Facility (RACF).

A.1 Configure WebLogic Open LDAP

To configure Open LDAP for STA, follow the steps below.

1. Go to the WebLogic console login screen using the HTTP (default is 7001) or HTTPS (default is 7002) port number you selected during STA installation.

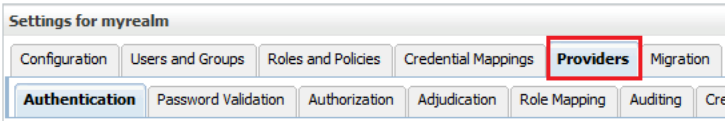
   http(s)://*yourHostName*:*PortNumber*/console/

2. Log in using the WebLogic Admin Console username and password you defined during STA installation.

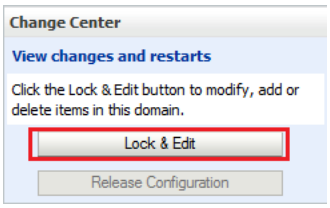
3. Under Domain Structure (left side of screen), click **Security Realms**.

4. Under Realms, select **myrealm** (select the name itself, not the check box).

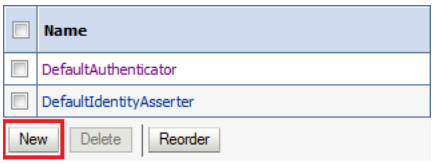
5. Click the **Providers** tab.



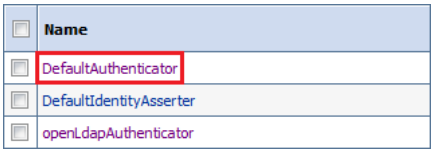
6. Under Change Center (top left of screen), click **Lock & Edit**.



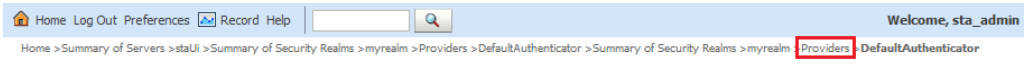
7. Under Authentication Providers, click **New**.



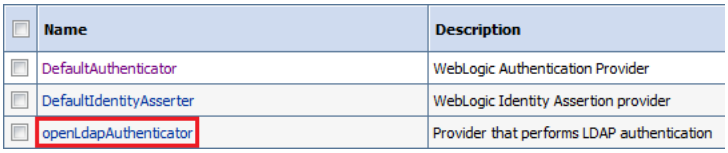
8. Enter the name of the authentication provider (for example, openLdapAuthenticator), and select **OpenLDAPAuthenticator** in the Type list. Click **OK**.
9. Select **DefaultAuthenticator** (select the name itself, not the check box).



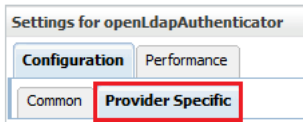
10. Change the **Control Flag** to Sufficient, and then click **Save**.
11. Click the **Providers** locator link (near top of screen) to return to the Authentication Providers screen.



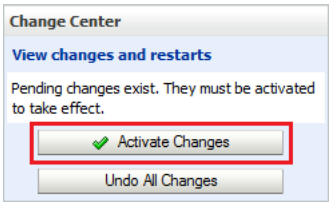
12. Under Authentication Providers, select the Open LDAP authenticator name you created in Step 8 (select the name itself, not the check box).



13. Change the **Control Flag** to Sufficient, and then click **Save**.
14. Click the **Provider Specific** tab.



15. Enter the following parameters. These settings apply to the lses-ldap1 server and are specific to each customer environment.
    - Host = lses-ldap1
    - Port = 389
    - Principal = leave blank
    - Credential = leave blank
    - User Base DN = ou=people,dc=oracle,dc=eng
    - User From Name Filter = (&(cn=%u)(objectclass=inetOrgPerson))
    - User Object Class = inetOrgPerson
    - Group Base DN = ou=groups,dc=oracle,dc=eng
    - Group From Name Filter = (&(cn=%g)(objectclass=groupofnames))
16. Click **Save**.
17. Under Change Center (top left of screen), click **Activate Changes**.



18. (Optional) Test the configuration by performing the following:
    a. Log out of the WebLogic console.
    b. Stop and restart STA using the `STA` command. For information on command usage, see the *STA Administration Guide*.

```
# STA stop all
# STA start all
```

    c. Log back in to the WebLogic console.
    d. Go to **Security Realms** > **myrealm** > **Users and Groups**.
    e. Within the **Users** and **Groups** tabs, verify entries exist in the Provider column for the Open LDAP provider.

A.2 Configure IBM RACF

To configure STA for RACF authentication, perform the following tasks:

- Task 1, "Review IBM RACF Mainframe Minimum Requirements"
- Task 2, "Enable Mainframe Support for STA RACF Authorization"
- Task 3, "Configure AT-TLS"
- Task 4, "Create the RACF Profiles Used by the CGI Routine"
- Task 5, "Import the Certificate File and Private Key File (Optional)"
- Task 6, "Test the CGI Routine"
- Task 7, "Set Up RACF/SSP for the WebLogic Console"

- Task 8, "Configure SSL Between STA and RACF"
- Task 9, "Configure the WebLogic Server"
- Task 10, "Install RACF/SSP on the WebLogic Console"

> **Note:** STA supports third-party products that are compatible with IBM RACF — for example, CA's ACF-2 and Top Secret. It is up to the person installing STA, or a security administrator, to issue the commands appropriate for the security product installed.

Task 1 Review IBM RACF Mainframe Minimum Requirements

RACF requirements are stated in the *STA Requirements Guide*.

Task 2 Enable Mainframe Support for STA RACF Authorization

The mainframe side of the RACF service for STA is provided by a CGI routine that is part of the SMC component for ELS 7.0 and 7.1. This CGI routine is called by the SMC HTTP server and uses RACF profiles defined in the FACILITY class.

For STA to use RACF as a means of access authentication, on the mainframe, you must set up an SMC Started Task that runs the HTTP server. You can find details on how to do this in the ELS document *Configuring and Managing SMC*.

> **Note:** The SMC Started Task must match the AT-TLS rule that has been defined. Alternately, allow the AT-TLS definition to use a generic jobname (for example, SMCW[1]).

[1] If you are using a value-supplied STC identifier (for example, JOBNAME.JOB), this will cause a CGI routine connection failure.

The port number used for the HTTP server must match the one defined in the WebLogic console, and the host must match the IP name for the host where the SMC task runs.

> **Note:** An existing SMC can be used if it exists on the host where RACF authorization is to be performed. In this case, use the port number of the existing HTTP server when you are performing the WebLogic configuration.

Task 3 Configure AT-TLS

AT-TLS is an encryption solution for TCP/IP applications that is transparent to the application server and client. Packet encryption and decryption occurs in the z/OS TCPIP address space at the TCP protocol level. AT-TLS requirements for RACF authorization are stated in the *STA Requirements Guide*.

The following RACF commands list the status of the various RACF objects that you will define in the configuration process:

- RLIST STARTED PAGENT.* STDATA ALL
- RLIST DIGTRING *ALL
- RLIST FACILITY IRR.DIGTCERT.LISTRING ALL
- RLIST FACILITY IRR.DIGCERT.LST ALL

- RLIST FACILITY IRR.DIGCERT.GENCERT ALL
- RACDCERT ID(stcuser) LIST
- RACDCERT ID(stcuser) LISTRING(keyringname)
- RACDCERT CERTAUTH LIST

To configure AT-TLS, do the following:

1. Activate AT-TLS

   Specify the following parameter in the TCPIP profile data set to activate the AT-TLS function:

   ```
   TCPCONFIG TTLS
   ```

   This statement may be placed in the TCP OBEY file.

2. Configure the Policy Agent (PAGENT)

   The Policy Agent address space controls which TCP/IP traffic is encrypted.

   a. Enter the PAGENT started task JCL.

      For example:

      ```
      //PAGENT PROC
      //*
      //PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
      // PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-d1'
      //*
      //STDENV DD DSN=pagentdataset,DISP=SHR//SYSPRINT DD SYSOUT=*
      //SYSOUT DD SYSOUT=*
      //*
      //CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
      ```

   b. Enter the PAGENT environment variables. The pagentdataset data set contains the PAGENT environment variables.

      For example:

      ```
      LIBPATH=/lib:/usr/lib:/usr/lpp/ldapclient/lib:.
      PAGENT_CONFIG_FILE=/etc/pagent.conf
      PAGENT_LOG_FILE=/tmp/pagent.log
      PAGENT_LOG_FILE_CONTROL=3000,2
      _BPXK_SETIBMOPT_TRANSPORT=TCPIP
      TZ=MST7MDT
      ```

      In this example, /etc/pagent.conf contains the PAGENT configuration parameters. Use your own time zone for the TZ parameter.

   c. Configure PAGENT.

      For example:

      ```
      TTLSRule TBI-TO-ZOS
      {
       LocalAddr localtcpipaddress
       RemoteAddr remotetcpipaddress
       LocalPortRange localportrange
       RemotePortRange remoteportrange
       Jobname HTTPserverJobname
       Direction Inbound
       Priority 255
       TTLSGroupActionRef gAct1~TBI_ICSF
      ```

```
 TTLSEnvironmentActionRef eAct1~TBI_ICSF
 TTLSConnectionActionRef cAct1~TBI_ICSF
}
TTLSGroupAction gAct1~TBI_ICSF
{
 TTLSEnabled On
 Trace 2
}
TTLSEnvironmentAction eAct1~TBI_ICSF
{
 HandshakeRole Server
 EnvironmentUserInstance 0
 TTLSKeyringParmsRef keyR~ZOS
}
TTLSConnectionAction cAct1~TBI_ICSF
{
 HandshakeRole ServerWithClientAuth
 TTLSCipherParmsRef cipher1~AT-TLS__Gold
 TTLSConnectionAdvancedParmsRef cAdv1~TBI_ICSF
 CtraceClearText Off
 Trace 2
}
TTLSConnectionAdvancedParms cAdv1~TBI_ICSF
{
 ApplicationControlled Off
 HandshakeTimeout 10
 ResetCipherTimer 0
 CertificateLabel certificatelabel
 SecondaryMap Off
}
TTLSKeyringParms keyR~ZOS
{
 Keyring keyringname
}
TTLSCipherParms cipher1~AT-TLS__Gold
{
 V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
 V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}
```

where:

– *localtcpipaddress*

  local TCP/IP address (address of HTTP server)

– *remotetcpipaddress*

  remote TCP/IP address (address of STA client). This can be ALL for all TCP/IP addresses

– *localportrange*

  local port of HTTP server (specified in the HTTP or SMC startup)

– *remoteportrange*

  remote port range (1024-65535 for all ephemeral ports)

– *HTTPserverJobname*

  jobname of the HTTP Server

– *certificatelabel*

label from certificate definition

– *keyringname*

name from RACF keyring definition

3. Activate RACF Classes

Enter the following commands to activate RACF classes. Either the RACF panels or the CLI can be used.

The RACF classes include:

- DIGTCERT
- DIGTNMAP
- DIGTRING

SERVAUTH CLASS must be RACLISTed to prevent PORTMAP and RXSERV from abending.

```
SETROPTS RACLIST(SERVAUTH)
RDEFINE SERVAUTH **UACC(ALTER) OWNER (RACFADM)
RDEFINE STARTED PAGENT*.* OWNER(RACFADM) STDATA(USER(TCPIP) GROUP(STCGROUP)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE) OWNER(RACFADM)
RDEFINE FACLITY IRR.DIGTCERT.LIST UACC(NONE) OWNER(RACFADM)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) OWNER (RACFADM)
```

4. Define RACF Keyrings and Certificates

a. Enter the following RACF commands to create Keyrings and certificates:

```
RACDCERT ID(stcuser) ADDRING(keyringname)
```

where:

* *stcuser*: RACF user id associated with the TCPIP address space
* *keyringname*: Name of the keyring, must match the Keyring specified in the PAGENT configuration

```
RACDCERT ID(stcuser) GENCERT CERTAUTH SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('calabel') TRUST
SIZE(1024) KEYUSAGE(HANDSHAKE,DATAENCRYPT,CERTSIGN)
```

Note: This is the CA certificate for the STA system.

where:

* *stcuser*: RACF user id associated with the TCPIP address space
* *serverdomainname*: Domain name of the z/OS server (for example, MVSA.COMPANY.COM)
* *companyname*: Organization name
* *unitname*: Organizational unit name
* *country*: Country
* *calabel*: Label for certificate authority (for example, CATBISERVER)

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('serverlabel')
TRUST SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Note: This is the SERVER certificate.

where:

* *stcuser:* RACF user id associated with the TCPIP address space
* *serverdomainname:* Domain name of the z/OS server (for example, MVSA.COMPANY.COM)
* *companyname:* Organization name
* *unitname:* Organizational unit name
* *country*: Country
* *serverlabel*: Label for the server certificate (for example, TBISERVER)
* *calabel:* Label for certificate authority, specified in the CA certificate definition

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('clientdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('clientlabel')
TRUST SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Note: This is the CLIENT certificate.

where:

* *stcuser*: RACF user id associated with the TCPIP address space
* *clientdomainname*: Domain name of the STA client (for example, TBIA.COMPANY.COM)
* *companyname*: Organization name
* *unitname*: Organizational unit name
* *country*: Country
* *clientlabel*: Label for the server certificate –TBICLIENT
* *calabel*: Label for certificate authority, specified in the CA certificate definition.

b. Enter the following commands to connect the CA, SERVER, and CLIENT certificates to the keyring specified in the PAGENT configuration:

```
RACDCERT ID(stcuser) CONNECT(CERTAUTH LABEL('calabel') RING('keyringname')
USAGE(CERTAUTH))
```

where:

* *stcuser*: RACF user id associated with the TCPIP address space
* *calabel:* Label for certificate authority, specified in the CA certificate definition
* *keyringname:* Name of the keyring, must match the Keyring specified in the PAGENT configuration

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('serverlabel')
RING('keyingname') DEFAULT USEAGE(PERSONAL)
```

where:

* *stcuser*: RACF user id associated with the TCPIP address space
* *serverlabel*: Label for the server certificate
* *keyringname*: Name of keyring, must match the Keyring specified in the PAGENT configuration

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('clientlabel')
RING('keyingname') USEAGE(PERSONAL)
```

where:

* *stcuser:* RACF user id associated with the TCPIP address space
* *clientlabel*: Label for the client certificate
* *keyringname*: Name of keyring, must match the Keyring specified in the PAGENT configuration

c. Enter the following commands to export the CA and client certificates to be transmitted to STA:

```
RACDCERT EXPORT (LABEL('calabel')) CERTAUTH DSN('datasetname')
FORMAT(CERTB64)
```

where:

* *calabel*: Label for certificate authority, specified in the CA certificate definition
* *datasetname:* Data set to receive the exported certificate

```
RACDCERT EXPORT (LABEL('clientlabel')) ID(stcuser) DSN('datasetname')
FORMAT(PKCS12DER) PASSWORD(' password ')
```

where:

* *clientlabel*: Label for the client certificate
* *stcuser*: RACF user id associated with the TCPIP address space
* *datasetname*: Data set to receive the exported certificate
* *password*: Password for data encryption. Needed when the certificate is received on STA. The password must be eight characters or more.

The export data sets are now transmitted to STA, and FTP can be used. The CA certificate is transmitted with an EBCDIC to ASCII conversion. The CLIENT certificate is transmitted as a BINARY file and contains both the client certificate and its private key.

Task 4 Create the RACF Profiles Used by the CGI Routine

The profiles are defined in the FACILITY class. The first of the profiles is called SMC.ACCESS.STA and determines whether a user has access to the STA application.

A user who requires access to STA must have READ access to this profile. The other profiles are all shown as SMC.ROLE.*nnn* and are used to determine which roles the user has once logged on.

Note: The only role defined to STA is StorageTapeAnalyticsUser. To obtain this role, you must request your userid to be added to the SMC.ROLE.STORAGETAPEANALYTICSUSER profile with READ access.

Task 5 Import the Certificate File and Private Key File (Optional)

This procedure can be valuable to test that public and private keys have been generated successfully and that user IDs and passwords with the appropriate permissions have been defined correctly.

The test can be done using any browser, but Firefox is used here as an example.

1. In Firefox, click **Tools** and then **Options**.
2. Select the **Advanced** tab and then the **Encryption** tab.
3. Click the **View Certificates** button.
4. Click the **Authorities** tab in the Certificate Manager dialog box, and then select the certificate file to import.
5. Click **Import**.
6. Click the **Your Certificates** tab, and then enter the private key file to import.
7. Click **Import**.
8. Click the **OK** button to save and exit the dialog box.

Task 6 Test the CGI Routine

To test the CGI routine from a browser, enter the following URL, where *host*, *port*, *userid*, and *password* are set to appropriate values.

https://*host*:*port*/smcgsaf?type=authentication&userid=*userid*

&password=*password*&roles=StorageTapeAnalyticsUser

The resultant output indicates whether or not the user is authorized to access STA and the StorageTapeAnalyticsUser role.

> **Note:** The STA RACF authorization facility does not support changing the password of mainframe user IDs. If a user ID password expires, STA indicates this, and the password must be reset through normal mainframe channels before attempting to log in to STA again.

Task 7 Set Up RACF/SSP for the WebLogic Console

The RACF Security Service Provider (or RACF SSP) must be installed as a plug-in into WebLogic.

If the RACF SSP has been installed, the STA installer should put the RACF SSP in the appropriate location within WebLogic. If it has not been installed, place the RACF security **jar** file into the directory named:

```
/Oracle/Middleware/wlserver_10.3/server/lib/mbeantypes/staRACF.jar
```

Task 8 Configure SSL Between STA and RACF

1. Install the required PTFs on the MVS system. These PTFs allow for authentication with RACF or other third-party security software when you are logging on to the STA. For PTF requirements, see the *STA Requirements Guide*.

   The Application Transparent TLS (AT-TLS) has been configured on MVS so that the port number defined to the SMC HTTP Server and WebLogic is encrypted to the server.

Before proceeding, ensure you possess two files: the MVS server certificate (in ASCII format) and the STA client private key (in binary PKCS12 format). The MVS system administrator has given you the password to the PKCS12 file.

2. Place the certificate in Oracle/Middleware/user_projects/domains/tbi/cert.
3. Convert the certificate from the DER format to the PEM format.

   openssl pkcs12 -clcerts -in PKCS12DR.*xxxxxx* **-out** *mycert***.pem**

   You will be asked to enter the Import Password (given to you with the certificate), a new PEM password, and password verification.
4. Using the Java keytool command, import the certificate file into the /Oracle/Middleware/jdk1.6.0_xx/jre/lib/security/cacerts file with the following command:

   ```
   /Oracle/Middleware/jdk1.6.0_xx/jre/bin/keytool -importcert -alias tbiServer
   -file certificate -keystore /Oracle/Middleware/jdk1.6.0_
   xx/jre/lib/security/cacerts -storetype jks
   ```

Task 9 Configure the WebLogic Server

To configure WebLogic for RACF authentication, follow the procedure in "Reconfigure WebLogic to use a Different Security Certificate" on page 8-2.

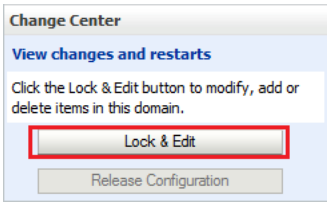
Task 10 Install RACF/SSP on the WebLogic Console

1. Go to the WebLogic console login screen using the HTTP (default is 7001) or HTTPS (default is 7002) port number you selected during STA installation.

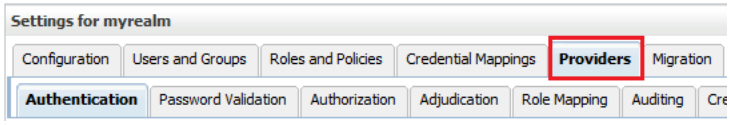
   http(s)://*yourHostName*:*PortNumber*/console/
2. Log in using the WebLogic Admin Console username and password you defined during STA installation.
3. Under Domain Structure (left side of screen), click **Security Realms**.

4. Under Realms, select **myrealm** (select the name itself, not the check box).

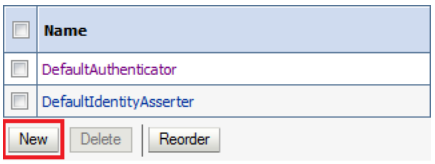
5. Under Change Center (top left of screen), click **Lock & Edit**.



6. Select the **Providers** tab.



7. Under Authentication Providers, click **New**.

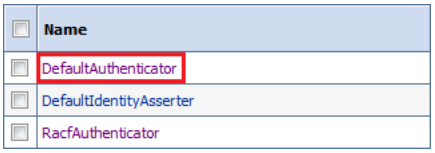


8. Enter the name of the authentication provider (for example, RacfAuthenticator) and select **RacfAuthenticator** in the Type list. Click **OK**.

   In the Type list, the RACF jar file should be listed. If it is not, stop and restart STA using the `STA` command. For information on command usage, see the *STA Administration Guide*.

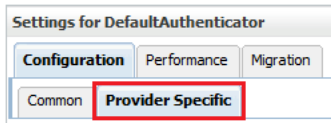
9. Under Authentication Providers, make sure the RACF provider is last in the list. The DefaultAuthenticator and DefaultIdentityAsserter must always be the first two items in this list.

10. Click **DefaultAuthenticator** (select the name itself, not the check box).

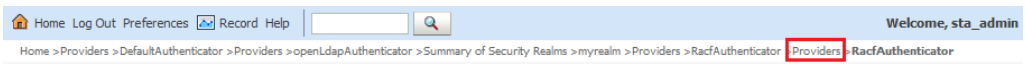


11. Change the Control Flag to Sufficient, and then click **Save**.

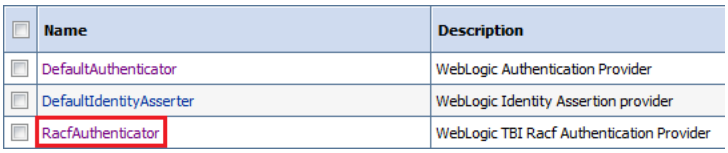
12. Select the **Provider Specific** tab, and then click **Save**.



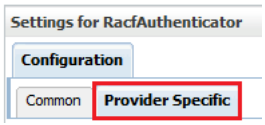
13. Click the **Providers** locator link to return to the Authentication Providers screen.



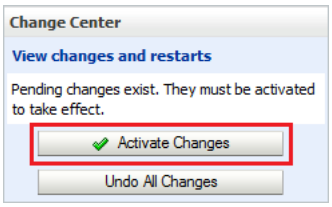
14. Under Authentication Providers, select the RACF authenticator name you created in Step 8 (select the name itself, not the check box).



15. Change the Control Flag to Sufficient, and then click **Save**.
16. Select the **Provider Specific** tab.



17. Enter the Host name (for example, mvshost.yourcompany.com) and Port number (for example, 8700) where the MVS system is running, and then click **Save**.
18. Under Change Center (top left of screen), click **Activate Changes**.



19. Log out of WebLogic.
20. Stop and restart STA using the `STA` command. For additional information on using the `STA` command, see the *STA Administration Guide*.

```
# STA stop all
# STA start all
```

B

Configuring SNMP v2c Mode

STA always attempts to communicate with libraries using the recommended SNMP v3 protocol. If v3 communication is not possible (for instance, if v3 is not configured on the library), STA will use v2c if enabled as per this appendix. Enable v2c mode if STA will be monitoring any libraries configured for v2c.

The SNMP v3 configuration process is described in Chapter 4, "Library Configuration Process," and Chapter 5, "Configuring SNMP in STA." The following sections describe the specific procedures that differ for v2c configuration.

B.1 SNMP v2c Mode Configuration Process

Use this procedure to configure STA and the libraries to use SNMP v2c for SNMP communications.

1. In Chapter 4, follow all procedures shown in Table 4–2, " Tasks to Configure Libraries for STA", except:
   - Replace "Create an SNMP v3 Trap Recipient" with Appendix B.2, "Create an SNMP v2c Trap Recipient."
   - After completing the process in Table 4–2, follow the procedure in Appendix B.3, "Enable SNMP v2c Mode for STA."
2. Follow the procedures in Chapter 5, "Configuring SNMP in STA".

B.2 Create an SNMP v2c Trap Recipient

Use this procedure to define the STA server as an authorized recipient of SNMP v2c traps and to define traps the library sends. You can use the CLI, SL Console, or SL150 browser interface, depending on library model. Note the following:

- Separate trap levels with commas.
- To avoid duplicate records, do not define the STA server as a trap recipient in multiple instances. For example, do not create both a v3 and v2c trap recipient definition for the STA server.
- Trap level 4 may not be supported by older library firmware versions; however, it can always be specified when creating a trap recipient.

- To avoid entry errors in the CLI, you can first type the command in a text file, and then copy and paste it into the CLI. For help with CLI commands, type `help snmp`.

With the CLI (All libraries except SL150)

1. Use the following command to create a v2c SNMP trap recipient.

   `snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45, 61,63,65,81,85,100 host` *`STA_server_IP`* **`version v2c community`** *`community_name`*

   STA_server_IP: The IP address of the STA server.

   community_name: The v2c trap community. This can be **public**, or another name.

Example B–1 SL500, SL3000, and SL8500

```
SL3000> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v2c
community public
```

2. List the trap recipients to verify the STA server has been added correctly.

   `snmp listTrapRecipients`

With the SL Console (SL500 libraries only)

1. From the menu, select **Tools** > **System Detail**.
2. In the left panel, select **Library**.
3. In the right panel, select **SNMP** > **Add Trap Recipients**.
4. Enter the following information:

   Host: IP address of the STA server.

   TrapLevel: Comma-separated list of trap levels the library should send to STA: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100

   Version: Select **v2c**.

   Community – This can be **public**, or another name.

5. Click **Apply** to add the trap recipient.

With the SL150 User Interface

1. Select **SNMP** from the navigation menu on the left side of the interface.
2. Under the SNMP Trap Recipients section (or tab), select **Add Trap Recipient**.
3. Complete the Add Trap Recipient fields as follows:

   Host Address: IP address of the STA server.

   Trap Level: Comma-separated list of trap levels the library should send to STA: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100

   Version: Select **v2c**.

   Community Name: Can be **public**, or another name.

4. Click **OK** to add the trap recipient.

B.3 Enable SNMP v2c Mode for STA

1. Establish a terminal session with the STA server and log in as root.
2. Change to the STA configuration files directory.

```
# cd /Oracle/Middleware/user_projects/domains/TBI
```

3. Edit the SNMP version properties file.

```
# vi TbiSnmpVersionSupport.properties
```

4. Ensure the value of the V2c parameter is set to **true**.

```
V2c=true
```

5. Save and exit the file.
6. If you changed the value of the V2c parameter in Step 4, stop and restart all STA processes.

```
# STA stop all
# STA start all
```

C

Configuration Troubleshooting

Use this appendix to troubleshoot connections between the STA server and the library.

Note: This appendix assumes you are using the recommended SNMP v3 protocol for STA communications.

C.1 Troubleshooting Connection Tests and Data Collections

Use the following sections to troubleshoot library connection tests (as described in "Test the SNMP Connection to the Library" on page 5-5) and "Get latest data" requests (as described in "Get the Latest Configuration Data From the Library" on page 5-6).

C.1.1 MIB Walk Channel Test

The MIB Walk Channel test checks for library initialization, network connectivity, proper SNMP client settings, and correct library firmware. If this test fails, one or more of the following could be true:

- STA is not configured
- The library is not initialized
- The library firmware does not meet the minimum for STA
- There are network problems between the STA server and library
- A static IP address is not assigned to the STA server or library
- SNMP is not enabled on the library
- SNMP client settings do not match between STA server and library

To resolve the failure, perform troubleshooting steps on both the library and STA server, as follows.

C.1.1.1 What to Check on the Library

1. Verify that the library is fully initialized (see "Verify the Library is Operational" on page 5-4).

2. Use the `traceroute` command to check communication between the library and server. (This command is not available on the SL150.)

   a. Log in to the library.

   b. Issue one of the following commands:

      – SL8500 and SL3000:

        `traceRoute` *`sta_server_IP_address`*

      – SL500:

        `traceroute` *`sta_server_IP_address`*

      The output shows the number of hops and the round-trip time to reach each hop. The round-trip time (the last line in the command output) should be less than one second. If it is not, confirm the network's performance with your network administrator.

3. Ensure that SNMP has been enabled on the public port (see "Enable SNMP on the Library" on page 4-6).

4. Verify that there is one and only one SNMP v2c user (see "Ensure an SNMP v2c User" on page 4-6).

5. Verify that the SNMP v3 user was added correctly:

   - On SL500, SL3000, and SL8500 libraries, use the `snmp listUsers` command to view a list of SNMP users. On SL150 libraries, go to **SNMP** > **SNMP Users**.
   - To create a v3 user, see "Create an SNMP v3 User" on page 4-8.

6. Ensure that a static IP address has been assigned to the library (see "Retrieve the Library IP Address" on page 4-4).

7. After performing all other steps on both the library and STA server, consider deleting and re-adding the SNMP v3 user.

C.1.1.2 What to Check on the Server

1. Ensure the STA server is using a static IP address.

2. Use the `traceroute` command to check communication between the server and library.

   a. Log in to the STA server.

   b. Issue the following command:

      `traceroute -I` *`library_IP_address_or_name`*

      The output shows the number of hops and the round-trip time to reach each hop. The round-trip time (the last line in the command output) should be less than one second. If it is not, confirm the network's performance with your network administrator.

3. Verify that the STA server can reach the library public port by pinging the primary IP address and, if applicable, the secondary IP address.

4. Verify that UDP ports 161 and 162 are enabled on all network nodes between the STA server and the library (see "Verify SNMP Communications With the Library" on page 5-1).

5. Display the STA SNMP Client Attributes screen, and verify that the settings exactly match the corresponding settings for the SNMP v3 user and SNMP v3 trap

recipient on the library (see "Configure SNMP Client Settings for STA" on page 5-2).

6. Display the STA Monitored Libraries screen, and verify that the settings are correct for the library (see "Configure SNMP Connections With the Library" on page 5-3).

C.1.2 Trap Channel Test

The Trap Channel test requests that the library send a test trap (13) to the STA server. If the test fails, STA will indicate the date and time when the last trap/inform was received. If the test fails or indicates "Unknown", one or more of the following could be true:

- The library firmware may not support the test trap
- The STA server may not be properly configured as a trap recipient on the library
- If you recently upgraded to STA 2.0.x, the STA server's IP address may not be specified in the connection details for the library.

To resolve:

1. Ensure the library is running the recommended (or higher) firmware shown in the *STA Requirements Guide*. Lower firmware versions may not support the test trap (13).
2. After upgrading to STA 2.0.x, ensure you have selected the STA server's IP address in the library's connection details. See Task 10, "Configure STA 2.0.x" on page 9-11.
3. Use the `snmp engineId` (for SL500 libraries) or `snmp engineId print` (for SL3000 and SL8500 libraries) command to display the library engine ID. (Not applicable to SL150 libraries.)
4. Verify that STA is correctly configured as a trap recipient (see "Create an SNMP v3 Trap Recipient" on page 4-9).

   On SL500, SL3000, and SL8500 libraries, use the `snmp listTrapRecipients` command to display a list of trap recipients on the library. On SL150 libraries, go to **SNMP** > **SNMP Trap Recipients**.

   - **Engine Id**: Must match the library engine ID displayed in Step 3. The entry must not contain any upper-case characters. For the SL8500 and SL3000 libraries, the entry must include the 0x prefix (the SL500 may also show this prefix).
   - **Host**: IP address of the STA server.
   - **Version**: Must be v3.
   - **Auth**: Must be SHA.
   - **Priv**: Must be DES.
   - **Auth Pass** and **Priv Pass**: Must match the passwords on the STA SNMP Client Attributes screen, as well as the passwords specified when creating an SNMP user. For SL500 libraries, verify the passwords do not contain single quotes as text.
   - **Trap Level**: Must include trap 13.
5. Verify that the library engine ID from Step 3 matches the value in the STA UI (**Setup & Administration** > **Configuration** > **SNMP Connections** > **Monitored Libraries**). If it does not match:

a. Select the library in the Monitored Libraries list.

b. Click the **Edit** button.

c. Clear the Library Engine ID field, and then click **Save**.

d. Perform a connection test to retrieve the library's engine ID (see "Test the SNMP Connection to the Library" on page 5-5).

C.1.3 Media Validation Support Test

The Media Validation Support test checks for the correct firmware and configuration to enable Media Validation in STA. If the library model does not support Media Validation, the test will report **Not Applicable**. If the test is unsuccessful for a library that can support Media Validation, one or more of the following could be true:

- The library firmware does not support Media Validation
- SNMP v3 is not configured
- There are no drives in the Media Validation pool
- There are no empty or reservable drives in the Media Validation pool

To resolve:

1. See the *STA Requirements Guide* for the minimum library and drive firmware required for Media Validation.
2. Ensure you have an SNMP v3 user configured on both the library and STA server, and have configured the STA server to be a trap recipient on the library. Review the SNMP configuration steps in Chapter 4 and Chapter 5.

See the *STA User's Guide* for more information about configuring Media Validation.

C.2 Unsuccessful Trap Processing

If traps are not being received by the STA host, or traps are not being processed by STA, perform the following.

1. Ensure the STA server is using a static IP address.
2. Within a separate terminal window on the STA server, enter the following command as root:

   ```
   # tcpdump -v host library-public-port
   ```

   - *library-public-port* is the IP address of the primary public port on the library (see "Retrieve the Library IP Address" on page 4-4 for the correct entry).
   - In the output, look for **.snmptrap** and **SNMPv3**. Network traffic for "Get Latest Data" requests will contain **.snmp**.
   - If there is activity on the library, but no traps are being received, then check the library trap recipient entry for accuracy (see "Trap Channel Test" on page C-3).
3. Ensure SNMP port 162 is available for STA.

   The STA trap listener processes traps through port 162. To troubleshoot communications over this port, do the following.

   1. Check the /Oracle/Middleware/user_projects/domains/tbi/servers/staAdapter/logs/staAdapter.log file for a "SEVERE" error, such as:

"SEVERE: SNMP Trap/Inform Listener Port 162 is NOT bindable. Stop the application currently bound to that port."

2. If port 162 is already in use, determine what process is using it:

```
# netstat -ap |grep -I snmp
# netstat -anp |grep ":162"
```

3. Follow the process associated with the port or check what services may have started during system boot.

```
# chkconfig --list
```

4. If snmpd or snmtrapd are running, then ensure that they are turned off permanently.

   a. Deconfigure SNMP services:

```
# chkconfig snmpd off
# chkconfig snmptrapd off
```

   b. Stop SNMP services:

```
# service snmptrapd stop
# service snmpd stop
```

   c. Stop and restart STA services:

```
# STA stop all
# STA start all
```

5. If some traps are being reported in the Notifications screen, ensure that all trap levels were specified when creating a trap recipient on the library. See "Create an SNMP v3 Trap Recipient" on page 4-9 for the list of supported trap levels.
6. For the SL500, ensure you configured the library with a supported version of SL Console. Earlier versions of SL Console restricted the number of trap level characters that could be entered.
7. For SL500 and SL150 libraries, ensure the Volume Label Format is set properly:
   - "Set the SL500 Volume Label Format" on page 4-11
   - "Set the SL150 Volume Label Format and Drive Element Addressing Mode" on page 4-12

Index

V